Środa, 17 kwietnia 2019 r.

P8_TA(2019)0421

Zapobieganie rozpowszechnianiu w internecie treści o charakterze terrorystycznym ***I

Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 17 kwietnia 2019 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym (COM(2018)0640 – C8-0405/2018 – 2018/0331(COD))

(Zwykła procedura ustawodawcza: pierwsze czytanie)

(2021/C 158/68)

Parlament Europejski,

— uwzględniając wniosek Komisji przedstawiony Parlamentowi Europejskiemu i Radzie (COM(2018)0640),

— uwzględniając art. 294 ust. 2 i art. 114 Traktatu o funkcjonowaniu Unii Europejskiej, zgodnie z którymi wniosek został przedstawiony Parlamentowi przez Komisję (C8-0405/2018),

— uwzględniając art. 294 ust. 3 Traktatu o funkcjonowaniu Unii Europejskiej,

— uwzględniając uzasadnioną opinię przedstawioną – na mocy protokołu nr 2 w sprawie stosowania zasad pomocniczości i proporcjonalności – przez Izbę Poselską Republiki Czeskiej, w której stwierdzono, że projekt aktu ustawodawczego nie jest zgodny z zasadą pomocniczości,

— uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego z dnia 12 grudnia 2018 r. ([1]),

— uwzględniając art. 59 Regulaminu,

— uwzględniając sprawozdanie Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych oraz opinie przedstawione przez Komisję Kultury i Edukacji i przez Komisję Rynku Wewnętrznego i Ochrony Konsumentów (A8-0193/2019),

1. przyjmuje poniższe stanowisko w pierwszym czytaniu;

2. zwraca się do Komisji o ponowne przekazanie mu sprawy, jeśli zastąpi ona pierwotny wniosek, wprowadzi w nim istotne zmiany lub planuje ich wprowadzenie;

3. zobowiązuje swojego przewodniczącego do przekazania stanowiska Parlamentu Radzie i Komisji oraz parlamentom narodowym.

P8_TC1-COD(2018)0331

Stanowisko Parlamentu Europejskiego przyjęte w pierwszym czytaniu w dniu 17 kwietnia 2019 r. w celu przyjęcia rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/… w sprawie ~~zapobiegania rozpowszechnianiu~~*zwalczania rozpowszechniania* w internecie treści o charakterze terrorystycznym [Popr. 1]

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 114,

uwzględniając wniosek Komisji Europejskiej,

([1]) Dz.U. C 110 z 22.3.2019, s. 67.

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego ([1]),

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą ([2]),

a także mając na uwadze, co następuje:

(1) Niniejsze rozporządzenie ma na celu zapewnienie sprawnego funkcjonowania jednolitego rynku cyfrowego w otwartym i demokratycznym społeczeństwie poprzez ~~zapobieganie~~ ***przeciwdziałanie*** wykorzystywaniu usług hostingowych do celów terrorystycznych ***oraz przyczynienie się do poprawy bezpieczeństwa publicznego w społeczeństwach europejskich***. Należy poprawić funkcjonowanie jednolitego rynku cyfrowego poprzez zwiększenie pewności prawa dla dostawców usług hostingowych, ~~podniesienie~~***zwiększenie*** zaufania użytkowników do środowiska internetowego oraz wzmocnienie gwarancji w odniesieniu do wolności wypowiedzi***, wolności otrzymywania*** i ***przekazywania*** informacji ***i idei w otwartym i demokratycznym społeczeństwie, a także wolności prasy i pluralizmu mediów***. **[Popr. 2]**

(1a) Rozporządzenie w sprawie dostawców usług hostingowych może jedynie uzupełniać strategie państw członkowskich mające na celu zwalczanie terroryzmu, które muszą kłaść nacisk na środki pozainternetowe, takie jak inwestycje w pracę społeczną, inicjatywy na rzecz deradykalizacji i współpraca z zainteresowanymi społecznościami, aby doprowadzić do trwałego zapobiegania radykalizacji w społeczeństwie. **[Popr. 3]**

(1b) Treści o charakterze terrorystycznym to część szerszego problemu nielegalnych treści w internecie, do których zaliczają się inne treści, np. treści dotyczące wykorzystywania seksualnego dzieci, nielegalnych praktyk handlowych i treści stanowiące naruszenie własności intelektualnej. Przemycanie nielegalnych treści jest często stosowane przez organizacje terrorystyczne i inne organizacje o charakterze przestępczym do prania pieniędzy i zwiększenia początkowego kapitału wykorzystywanego do finansowania ich działań. Problem ten wymaga połączenia środków o charakterze ustawodawczym, nieustawodawczym i dobrowolnym, opartych na współpracy między organami a dostawcami usług, przy pełnym poszanowaniu praw podstawowych. **[Popr. 4]**

(2) Dostawcy usług hostingowych działający w internecie odgrywają zasadniczą rolę w gospodarce cyfrowej, łącząc przedsiębiorstwa i obywateli***, zapewniając możliwości uczenia się*** oraz ułatwiając publiczną debatę oraz dystrybucję i otrzymywanie informacji, opinii i pomysłów, co znacząco przyczynia się do innowacji, wzrostu gospodarczego i tworzenia miejsc pracy w Unii. Ich usługi są jednak w niektórych przypadkach wykorzystywane przez osoby trzecie w celu prowadzenia nielegalnej działalności w internecie. Szczególnie niepokojące jest wykorzystywanie dostawców usług hostingowych przez grupy terrorystyczne i ich zwolenników do rozpowszechniania w internecie treści o charakterze terrorystycznym w celu szerzenia swojego przesłania, radykalizacji i rekrutacji oraz ułatwiania działalności terrorystycznej i kierowania nią. **[Popr. 5]**

(3) Obecność treści o charakterze terrorystycznym w internecie ~~ma~~***okazała się decydującym, choć nie jedynym, czynnikiem sprzyjającym radykalizacji osób, które dopuściły się aktów terrorystycznych, co miało*** poważne negatywne konsekwencje dla ~~użytkowników,~~ obywateli i ogółu społeczeństwa, ~~jak również~~***a także*** dla dostawców usług online, u których zamieszczane są tego rodzaju treści, ponieważ podważa zaufanie ich użytkowników i szkodzi ich modelom biznesowym. W ~~świetle~~***związku z*** ich ~~centralnej roli~~ ***kluczową rolą*** oraz ***proporcjonalnie do*** środków technologicznych i zdolności związanych ze świadczonymi przez nich usługami dostawcy usług internetowych mają ~~szczególne~~ obowiązki społeczne dotyczące ochrony swoich usług przed wykorzystaniem przez terrorystów i pomocy ***właściwym organom*** w zwalczaniu ~~treści~~***przestępstw*** o charakterze terrorystycznym ~~rozpowszechnianych~~ ***popełnianych*** za pośrednictwem ich usług***, z jednoczesnym uwzględnieniem podstawowego znaczenia wolności wypowiedzi oraz wolności otrzymywania i przesyłania informacji i idei w otwartym i demokratycznym społeczeństwie***. **[Popr. 6]**

([1]) Dz.U. C 110 z 22.3.2019, s. 67.
([2]) Stanowisko Parlamentu Europejskiego z dnia 17 kwietnia 2019 r.

Środa, 17 kwietnia 2019 r.

(4) Należy uzupełnić ramy dobrowolnej współpracy między państwami członkowskimi a dostawcami usług hostingowych, poprzez które w 2015 r. zainicjowano wysiłki na poziomie Unii Europejskiej w celu zwalczania treści o charakterze terrorystycznym w internecie, jasnymi ramami prawnymi, aby dalej ograniczyć dostępność treści o charakterze terrorystycznym w internecie i odpowiednio rozwiązać ten szybko narastający problem. Ramy prawne, zgodnie z założeniem, mają opierać się na dobrowolnych wysiłkach, które zostały wzmocnione zaleceniem Komisji (UE) 2018/334 ([3]), i stanowią odpowiedź na wezwania Parlamentu Europejskiego do wzmocnienia środków zwalczania nielegalnych i szkodliwych treści ***zgodnie z ramami horyzontalnymi ustanowionymi na mocy dyrektywy 2000/31/WE*** oraz na wezwania Rady Europejskiej do usprawnienia ~~automatycznego~~ wykrywania i usuwania treści, które podżegają do aktów terrorystycznych. **[Popr. 7]**

(5) Stosowanie niniejszego rozporządzenia nie powinno mieć wpływu na stosowanie ~~art. 14~~ dyrektywy 2000/31/WE ([4]). ~~W szczególności wszelkie środki wprowadzone przez dostawcę usług hostingowych zgodnie z niniejszym rozporządzeniem, w tym wszelkie proaktywne środki, nie powinny same w sobie prowadzić do utraty przez dostawcę usług zwolnienia od odpowiedzialności przewidzianego w tym przepisie~~. Niniejsze rozporządzenie nie wpływa na uprawnienia organów i sądów krajowych do ustalenia odpowiedzialności dostawców usług hostingowych w szczególnych przypadkach, gdy nie są spełnione warunki wyłączenia odpowiedzialności na podstawie ~~art. 14~~ dyrektywy 2000/31/WE. **[Popr. 8]**

(6) Zasady mające na celu ~~zapobieganie wykorzystywaniu~~***zwalczanie wykorzystywania*** usług hostingowych do rozpowszechniania w internecie treści o charakterze terrorystycznym, aby zagwarantować sprawne funkcjonowanie rynku wewnętrznego, zostały określone w niniejszym rozporządzeniu ~~przy pełnym poszanowaniu praw podstawowych chronionych~~***i powinny być w pełni zgodne z prawami podstawowymi objętymi ochroną*** w unijnym porządku prawnym, a zwłaszcza ~~praw gwarantowanych~~***z prawami gwarantowanymi*** w Karcie praw podstawowych Unii Europejskiej. **[Popr. 9]**

(7) Niniejsze rozporządzenie ~~przyczynia~~***ma na celu przyczynienie*** się do ochrony bezpieczeństwa publicznego~~, a jednocześnie ustanawia~~ ***i powinno ustanowić*** odpowiednie i solidne gwarancje zapewniające ochronę odnośnych praw podstawowych. Obejmuje to prawo do poszanowania życia prywatnego i do ochrony danych osobowych, prawo do skutecznej ochrony sądowej, prawo do wolności wypowiedzi, w tym wolność otrzymywania i przekazywania informacji, prawo do wolności prowadzenia działalności gospodarczej oraz zasadę niedyskryminacji. Właściwe organy i dostawcy usług hostingowych powinni przyjmować wyłącznie środki, które są konieczne, ~~odpowiednie~~ i proporcjonalne w ~~ramach społeczeństwa demokratycznego~~***społeczeństwie demokratycznym***, biorąc pod uwagę szczególne znaczenie, jakie ma wolność wypowiedzi ***oraz wolność otrzymywania*** i ***przekazywania*** informacji ***i idei***, ***a także prawo do poszanowania życia prywatnego i rodzinnego oraz ochrona danych osobowych, które stanowią podstawowe fundamenty pluralistycznego***~~, która jest jednym z podstawowych fundamentów pluralistycznego społeczeństwa~~ demokratycznego ***społeczeństwa*** oraz ~~jedną z~~***należą do*** wartości, na których opiera się Unia. ~~Środki stanowiące ingerencję~~***Bez względu na rodzaj środków należy unikać ingerencji*** w wolność wypowiedzi i informacji***, a środki te powinny także w miarę możliwości*** ~~powinny być ściśle ukierunkowane w tym sensie, że muszą one~~ służyć ~~zapobieganiu rozpowszechnianiu~~***zwalczaniu rozpowszechniania*** treści o charakterze terrorystycznym ***poprzez zastosowanie ściśle ukierunkowanego podejścia***, lecz nie mogą wywierać wpływu na prawo do zgodnego z prawem otrzymywania i udzielania informacji, z uwzględnieniem centralnej roli dostawców usług hostingowych w ułatwianiu debaty publicznej oraz w rozpowszechnianiu i przyjmowaniu faktów, opinii i pomysłów zgodnie z prawem. ***Skuteczne środki zwalczania terroryzmu w internecie oraz ochrona wolności wypowiedzi nie stanowią sprzecznych ze sobą celów, lecz uzupełniają się i wzajemnie się wzmacniają.*** **[Popr. 10]**

(8) Prawo do skutecznego środka odwoławczego zapisano w art. 19 TUE i art. 47 Karty praw podstawowych Unii Europejskiej. Każda osoba fizyczna lub prawna ma prawo do skutecznego środka ochrony prawnej przed właściwym sądem krajowym przeciwko wszelkim środkom wprowadzonym na podstawie niniejszego rozporządzenia, które mogą negatywnie wpłynąć na prawa tej osoby. Prawo to obejmuje w szczególności

([3]) Zalecenie Komisji (UE) 2018/334 z dnia 1 marca 2018 r. w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w internecie (Dz.U. L 63 z 6.3.2018, s. 50).

([4]) Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz.U. L 178 z 17.7.2000, s. 1).

możliwość skutecznego zaskarżenia nakazów usunięcia przez dostawców usług hostingowych i dostawców treści przed sądem państwa członkowskiego, którego organy wydały nakaz usunięcia ***oraz możliwość zaskarżenia przez dostawców treści środków podjętych przez dostawcę usług hostingowych***. **[Popr. 11]**

(9) W celu zapewnienia jasności w odniesieniu do działań, które zarówno dostawcy usług hostingowych, jak i właściwe organy powinny podejmować, aby ~~zapobiegać rozpowszechnianiu~~***zwalczać rozpowszechnianie*** w internecie treści o charakterze terrorystycznym, w niniejszym rozporządzeniu należy w celach prewencyjnych ustanowić definicję treści o charakterze terrorystycznym w oparciu o definicję przestępstw terrorystycznych na podstawie dyrektywy Parlamentu Europejskiego i Rady (UE) 2017/541 ([5]). Z uwagi na potrzebę ~~przeciwdziałania~~***zwalczania*** najbardziej ~~szkodliwej propagandzie terrorystycznej~~***szkodliwych treści o charakterze terrorystycznym*** w internecie definicja powinna obejmować materiały ~~i informacje~~, które podżegają, zachęcają lub nakłaniają do popełniania przestępstw terrorystycznych lub do ich wspierania~~, a także dostarczają instrukcji dotyczących popełniania~~ ***lub propagują udział w działaniach grupy terrorystycznej***, ***grożąc tym, że dojdzie do zamierzonego popełnienia jednego lub większej liczby*** takich przestępstw ~~lub propagują udział w działaniach grupy terrorystycznej~~. ***Definicja powinna obejmować także treści, które zawierają wskazówki dotyczące wytwarzania i stosowania materiałów wybuchowych, broni palnej lub jakichkolwiek innych rodzajów broni bądź substancji szkodliwych lub niebezpiecznych, jak również substancji chemicznych, biologicznych, radiologicznych i jądrowych (CBRJ), oraz wszelkie wskazówki dotyczące innych metod i technik, w tym w zakresie wyboru celów, które to wskazówki mają służyć popełnianiu przestępstw terrorystycznych.*** Informacje takie obejmują w szczególności tekst, obrazy, nagrania dźwiękowe i nagrania wideo. Oceniając, czy treści stanowią treści o charakterze terrorystycznym w rozumieniu niniejszego rozporządzenia, właściwe organy oraz dostawcy usług hostingowych powinni uwzględniać takie czynniki, jak charakter i treść oświadczeń, kontekst, w jakim oświadczenia zostały sporządzone, oraz to, w jakim stopniu mogą spowodować szkodliwe skutki, a tym samym wpływ na bezpieczeństwo i ochronę osób. Ważny czynnik w tej ocenie stanowi fakt, że dany materiał został wytworzony przez wymienioną w wykazie UE organizację terrorystyczną lub osobę, można go przypisać takiej organizacji lub osobie lub jest rozpowszechniany w imieniu takiej organizacji lub osoby. Treści rozpowszechniane w celach edukacyjnych, dziennikarskich lub badawczych ***bądź w celu zwiększenia świadomości z myślą o przeciwdziałaniu działalności terrorystycznej*** powinny być odpowiednio chronione. ***Zwłaszcza w przypadkach gdy dostawca treści ponosi odpowiedzialność redakcyjną, wszelkie decyzje o usunięciu rozpowszechnianych materiałów powinny uwzględniać standardy dziennikarskie ustanowione na podstawie przepisów dotyczących prasy lub mediów zgodnych z prawem Unii i Kartą praw podstawowych.*** Ponadto wyrażanie radykalnych, polemicznych lub kontrowersyjnych poglądów w ramach debaty publicznej na drażliwe kwestie polityczne nie powinno być uznawane za treści o charakterze terrorystycznym. **[Popr. 12]**

(10) Aby objąć te internetowe usługi hostingowe, w ramach których rozpowszechniane są treści o charakterze terrorystycznym, niniejsze rozporządzenie powinno mieć zastosowanie do usług społeczeństwa informacyjnego, w ramach których przechowuje się informacje dostarczone przez usługobiorcę na jego wniosek i udostępnia przechowywane informacje ~~osobom trzecim~~***społeczeństwu***, niezależnie od tego, czy działalność ta ma charakter czysto techniczny, automatyczny i bierny. Przykładowo do tego rodzaju dostawców usług społeczeństwa informacyjnego można zaliczyć: platformy mediów społecznościowych, transmisję strumieniową wideo, usługi wymiany materiałów wideo, audio i obrazów, wymianę plików i inne usługi w chmurze w zakresie, w jakim udostępniają one informacje ~~osobom trzecim~~***społeczeństwu***, i strony internetowe, na których użytkownicy mogą zamieszczać komentarze lub recenzje. Rozporządzenie to powinno mieć również zastosowanie do dostawców usług hostingowych mających miejsce prowadzenia działalności poza Unią, ale świadczących usługi na terytorium Unii, ponieważ znaczna część dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym w ramach swoich usług ma miejsce prowadzenia działalności w państwach trzecich. Powinno to zapewnić spełnianie tych samych wymogów przez wszystkie przedsiębiorstwa działające na jednolitym rynku cyfrowym, niezależnie od ich państwa prowadzenia działalności. Ustalenie, czy dostawca usług oferuje usługi w Unii, wymaga przeprowadzenia oceny, czy dostawca usług umożliwia korzystanie ze swoich usług osobom prawnym lub fizycznym w jednym lub kilku państwach członkowskich. Sama tylko dostępność strony internetowej dostawcy usług lub adresu poczty elektronicznej oraz innych danych kontaktowych w jednym lub kilku państwach członkowskich nie powinna być jednak warunkiem wystarczającym do objęcia zakresem zastosowania niniejszego rozporządzenia. ***Niniejsze rozporządzenie nie powinno mieć zastosowania do usług w chmurze, w tym usług w chmurze między przedsiębiorstwami, do których dostawca usług nie ma praw umownych w odniesieniu do***

([5]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW (Dz.U. L 88 z 31.3.2017, s. 6).

przechowywanych treści ani sposobu ich przetwarzania lub udostępniania publicznego przez klientów lub użytkowników końcowych tych klientów, a także w przypadku których dostawca usług nie ma możliwości technicznych usuwania konkretnych treści przechowywanych przez jego klientów lub ich użytkowników końcowych. **[Popr. 13]**

(11) Dla określenia zakresu niniejszego rozporządzenia powinien mieć znaczenie ścisły związek z Unią. Taki ścisły związek z Unią powinno się stwierdzać, jeżeli dostawca usług ma miejsce prowadzenia działalności w Unii lub, jeśli nie, ścisły związek ustala się, jeżeli znaczna liczba użytkowników ulokowana jest w co najmniej jednym państwie członkowskim lub jeżeli działalność jest ukierunkowania na co najmniej jedno państwo członkowskie. To, czy działalność jest kierowana do jednego lub większej liczby państw członkowskich, można ustalić na podstawie wszelkich istotnych okoliczności, w tym takich czynników, jak stosowanie języka lub posługiwanie się walutą danego państwa członkowskiego ~~lub możliwość składania zamówień na towary lub usługi~~. Kierowanie działalności do któregoś z państw członkowskich może również wynikać z dostępności aplikacji w danym krajowym sklepie z aplikacjami, z obecności reklam na rynku lokalnym lub z posługiwania się w reklamach językiem stosowanym w tym państwie członkowskim, lub z zarządzania relacjami z klientem polegającego np. na obsłudze klientów w języku powszechnie używanym w tym państwie członkowskim. W przypadku gdy usługodawca kieruje swoją działalność do jednego lub kilku państw członkowskich, jak określono w art. 17 ust. 1 lit. c) rozporządzenia (WE) nr 1215/2012 Parlamentu Europejskiego i Rady ([6]), należy również założyć ścisły związek. Z drugiej strony, świadczenie usługi w związku ze zwykłym przestrzeganiem zakazu dyskryminacji ustanowionego w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2018/302 ([7]) nie może być samo w sobie uważane za kierowanie lub ukierunkowywanie działalności na dane terytorium w Unii. **[Popr. 14]**

(12) Dostawcy usług hostingowych powinni dopełniać określonych obowiązków w zakresie staranności, aby ~~zapobiec rozpowszechnianiu~~***zwalczać rozpowszechnianie*** treści o charakterze terrorystycznym w ramach swoich usług ***dla społeczeństwa***. Te obowiązki w zakresie staranności nie powinny ~~sprowadzać się do~~***stanowić ogólnego obowiązku monitorowania przez dostawców usług hostingowych informacji, które przechowują, ani*** ogólnego obowiązku ~~monitorowania~~***aktywnego poszukiwania faktów lub okoliczności wskazujących na nielegalną działalność***. Obowiązki w zakresie staranności obejmują przy stosowaniu przez dostawców usług hostingowych niniejszego rozporządzenia ***przejrzystość,*** zachowanie przez nich należytej staranności, proporcjonalności i niedyskryminowania w działaniach wobec przechowywanych przez nich treści, w szczególności przy wdrażaniu własnych warunków w celu uniknięcia usuwania treści, które nie są treściami o charakterze terrorystycznym. Usuwanie lub uniemożliwianie dostępu musi odbywać się z poszanowaniem wolności wypowiedzi***, wolności otrzymywania*** i ***przesyłania*** informacji ***i idei w otwartym i demokratycznym społeczeństwie, a także wolności i pluralizmu mediów***. **[Popr. 15]**

(13) Procedura i obowiązki wynikające ze skierowanych do dostawców usług hostingowych nakazów usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do nich po przeprowadzeniu oceny przez właściwe organy powinny zostać zharmonizowane. Państwa członkowskie powinny zachować swobodę wyboru właściwych organów, która ~~umożliwi~~***umożliwia*** im wyznaczenie w tym celu ~~organów administracyjnych, organów ścigania~~***organu sądowego***, ***niezależnego organu administracyjnego*** lub ~~organów sądowych~~***organu ścigania***. Biorąc pod uwagę prędkość, z jaką treści o charakterze terrorystycznym są rozpowszechniane w internecie, przepis ten nakłada na dostawców usług hostingowych obowiązek zapewnienia usunięcia treści o charakterze terrorystycznym zidentyfikowanych w nakazie usunięcia lub uniemożliwienia dostępu do nich w ciągu ~~jednej~~ godziny od otrzymania nakazu usunięcia. ~~To do dostawców usług hostingowych należy decyzja, czy usunąć dane treści, czy też uniemożliwić dostęp do tych treści użytkownikom w Unii~~. **[Popr. 16]**

(14) Właściwy organ powinien przekazać nakaz usunięcia bezpośrednio ~~adresatowi i~~ punktowi kontaktowemu ***dostawcy usług hostingowych, a w przypadku dostawcy usług hostingowych posiadającego główną siedzibę w innym państwie członkowskim – właściwemu organowi tego państwa,*** za pomocą dowolnego środka elektronicznego zdolnego do sporządzenia pisemnego rejestru na warunkach, które umożliwiają dostawcy usług ustalenie autentyczności, w tym dokładności daty i czasu wysłania i otrzymania nakazu, np. za pośrednictwem zabezpieczonej poczty elektronicznej i platform lub innych zabezpieczonych kanałów, w tym udostępnionych

([6]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1215/2012 z dnia 12 grudnia 2012 r. w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych (Dz.U. L 351 z 20.12.2012, s. 1).

([7]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/302 z dnia 28 lutego 2018 r. w sprawie nieuzasadnionego blokowania geograficznego oraz innych form dyskryminacji klientów ze względu na przynależność państwową, miejsce rezydowania lub miejsce prowadzenia działalności na rynku wewnętrznym oraz w sprawie zmiany rozporządzeń (WE) nr 2006/2004 oraz (UE) 2017/2394 i dyrektywy 2009/22/WE (Dz.U. L 601 z 2.3.2018, s. 1.).

przez dostawcę usług, zgodnie z przepisami dotyczącymi ochrony danych osobowych. Wymóg ten może w szczególności zostać spełniony poprzez korzystanie z kwalifikowanych usług rejestrowanego doręczenia elektronicznego zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 910/2014 ([8]). **[Popr. 17]**

~~(15) Zgłoszenia dokonywane przez właściwe organy lub Europol stanowią skuteczny i szybki sposób informowania dostawców usług hostingowych o konkretnych treściach w ramach świadczonych przez nich usług. Mechanizm powiadamiania dostawców usług hostingowych o informacjach, które mogą być uznawane za treści o charakterze terrorystycznym, w celu dobrowolnego rozważenia przez dostawcę zgodności z jego własnymi warunkami powinien pozostać dostępny jako uzupełnienie nakazów usunięcia. Ważne jest, aby dostawcy usług hostingowych traktowali ocenę takich zgłoszeń priorytetowo i przekazywali szybkie informacje zwrotne na temat podjętych działań. Ostateczna decyzja dotycząca tego, czy usunąć dane treści, ponieważ nie są zgodne z warunkami dostawcy usług hostingowych, pozostaje w jego gestii. Wdrażając niniejsze rozporządzenie w odniesieniu do zgłoszeń, mandat Europolu, określony w rozporządzeniu (UE) 2016/794 ([9]), pozostaje niezmieniony.~~ **[Popr. 18]**

(16) Ze względu na skalę i tempo niezbędne do skutecznego identyfikowania i usuwania treści o charakterze terrorystycznym istotnym elementem w zwalczaniu treści o charakterze terrorystycznym w internecie są proporcjonalne ~~proaktywne~~ środki ***szczególne***~~, w tym~~ w ~~niektórych przypadkach środki zautomatyzowane. W~~ celu zmniejszenia dostępności treści o charakterze terrorystycznym w ramach świadczonych przez siebie usług dostawcy usług hostingowych powinni ocenić, czy należy wprowadzić ~~proaktywne~~ środki, ***szczególne*** w zależności od ~~zagrożenia~~***ryzyka*** i poziomu narażenia na treści o charakterze terrorystycznym, a także od wpływu ***otrzymywania i przesyłania informacji*** na prawa osób trzecich i ~~interesu publicznego danych informacji~~***interes publiczny, w szczególności jeżeli występuje znaczny poziom narażenia na treści o charakterze terrorystycznym i wpływa wiele nakazów usunięcia***. W związku z tym dostawcy usług hostingowych powinni określić, jakie odpowiednie***, celowe***, skuteczne i proporcjonalne ~~proaktywne~~ środki ***szczególne*** powinny zostać wdrożone. Wymóg ten nie powinien oznaczać ogólnego obowiązku monitorowania. ***Środki szczególne, o których mowa powyżej, mogą obejmować regularne sprawozdania dla właściwych organów, zwiększenie zasobów ludzkich zajmujących się środkami ochrony usług przed publicznym rozpowszechnianiem treści o charakterze terrorystycznym oraz wymianę najlepszych praktyk.*** W kontekście tej oceny brak nakazów usunięcia ~~i zgłoszeń~~ skierowanych do dostawcy usług hostingowych wskazuje na niski poziom narażenia na treści o charakterze terrorystycznym. **[Popr. 19]**

(17) Przy wprowadzaniu ~~proaktywnych~~ środków ***szczególnych*** dostawcy usług hostingowych powinni zapewnić zachowanie ~~prawa~~***przez*** użytkowników ***prawa*** do wolności wypowiedzi ***oraz wolności otrzymywania*** i ~~informacji~~ – ~~w tym prawa do swobodnego otrzymywania~~ ***przekazywania informacji i idei w otwartym*** i ~~przekazywania informacji~~ ***demokratycznym społeczeństwie***. Oprócz wszelkich wymogów określonych w prawie, w tym również w przepisach dotyczących ochrony danych osobowych, dostawcy usług hostingowych powinni działać z należytą starannością i wdrażać gwarancje, w tym w szczególności ~~w stosownych przypadkach~~ nadzór i weryfikacje przez człowieka, aby uniknąć jakichkolwiek niezamierzonych i błędnych decyzji prowadzących do usunięcia treści, które nie są treściami o charakterze terrorystycznym. ~~Ma to szczególne znaczenie, gdy dostawcy usług hostingowych wykorzystują zautomatyzowane sposoby wykrywania treści o charakterze terrorystycznym. Wszelkie decyzje o zastosowaniu zautomatyzowanych środków, niezależnie od tego, czy zostały podjęte przez samego dostawcę usług hostingowych czy na wniosek właściwego organu, powinny być oceniane pod kątem wiarygodności wykorzystanej technologii i wpływu na prawa podstawowe~~. **[Popr. 20]**

(18) W celu zapewnienia, aby dostawcy usług hostingowych narażeni na treści o charakterze terrorystycznym wprowadzali odpowiednie środki, by zapobiegać takiemu wykorzystywaniu świadczonych przez nich usług, ~~właściwe organy powinny~~***właściwy organ powinien*** zwrócić się do dostawców usług hostingowych, którzy otrzymali ~~nakaz usunięcia, który stał się prawomocny~~***naczną liczbę prawomocnych nakazów usunięcia***, z wnioskiem o przedstawienie informacji na temat przyjętych ~~proaktywnych~~ środków ***szczególnych***. ~~Mogłyby one obejmować środki zapobiegające ponownemu zamieszczeniu treści o charakterze terrorystycznym, które zostały usunięte lub do których dostęp został uniemożliwiony w wyniku otrzymania przez dostawców nakazu usunięcia lub zgłoszenia, przeprowadzające kontrolę w stosunku do narzędzi publicznych lub prywatnych zawierających znane~~

([8]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.U. L 257 z 28.8.2014, s. 73).

~~([9]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW (Dz.U. L 135 z 24.5.2016, s. 53).~~

~~treści o charakterze terrorystycznym. Mogą one~~***Może on*** również wykorzystywać wiarygodne narzędzia techniczne do identyfikacji nowych treści o charakterze terrorystycznym~~, dostępne na rynku albo opracowane przez dostawcę usług hostingowych~~. Dostawca usług powinien przedstawić sprawozdanie na temat wprowadzonych ~~szczególnych proaktywnych~~ środków ***szczególnych***, aby umożliwić właściwemu organowi ocenę, czy środki te są ***konieczne,*** skuteczne i proporcjonalne oraz czy, w razie wykorzystywania środków automatycznych, dostawca usług hostingowych posiada niezbędne umiejętności w zakresie nadzoru i weryfikacji przez człowieka. Oceniając skuteczność***, konieczność*** i proporcjonalność środków, właściwe organy powinny uwzględnić odpowiednie parametry, w tym liczbę nakazów usunięcia ~~i zgłoszeń~~ skierowanych do dostawcy, jego ***wielkość i*** zdolność ekonomiczną oraz wpływ jego usług na rozpowszechnianie treści o charakterze terrorystycznym (na przykład biorąc pod uwagę liczbę użytkowników w Unii)***, a także gwarancje wprowadzone w celu ochrony wolności wypowiedzi i informacji oraz liczbę przypadków ograniczenia legalnych treści***. **[Popr. 21]**

(19) Po wystąpieniu z wnioskiem właściwy organ powinien nawiązać z dostawcą usług hostingowych dialog na temat koniecznych ~~proaktywnych środków~~***środków szczególnych***, które należy wdrożyć. W razie konieczności właściwy organ powinien ~~narzucić przyjęcie~~ ***zwrócić się do dostawcy usług hostingowych o dokonanie ponownej oceny niezbędnych środków lub żądać przyjęcia*** odpowiednich, skutecznych i proporcjonalnych ~~proaktywnych środków~~***środków szczególnych***, jeżeli uzna, że dotychczas przyjęte środki ***nie są zgodne z zasadą konieczności i proporcjonalności lub*** są niewystarczające, by wyeliminować zagrożenie. ~~Decyzja o narzuceniu takich szczególnych proaktywnych środków nie powinna co do zasady prowadzić do nałożenia ogólnego obowiązku monitorowania, określonego w art. 15 ust. 1 dyrektywy 2000/31/WE. Biorąc pod uwagę szczególnie poważne zagrożenia związane z rozpowszechnianiem treści o charakterze terrorystycznym, decyzje przyjęte przez właściwe organy na podstawie niniejszego rozporządzenia mogą stanowić odstępstwo od podejścia ustanowionego~~ ***Właściwy organ powinien nakładać wyłącznie takie środki szczególne, których wdrożenia można rozsądnie oczekiwać od dostawcy usług hostingowych, biorąc pod uwagę, między innymi, zasoby finansowe i inne zasoby tego dostawcy. Żądanie wdrożenia takich środków szczególnych nie powinno prowadzić do nałożenia ogólnego obowiązku monitorowania określonego*** w art. 15 ust. 1 dyrektywy 2000/31/WE ~~w odniesieniu do niektórych szczególnych, ukierunkowanych środków, których przyjęcie jest niezbędne z uwagi na nadrzędne względy bezpieczeństwa publicznego. Przed przyjęciem takich decyzji właściwy organ powinien zachować równowagę między celami dotyczącymi interesu publicznego a odnośnymi prawami podstawowymi, w tym w szczególności wolnością wypowiedzi i informacji oraz wolnością prowadzenia działalności gospodarczej, a także przedstawić odpowiednie uzasadnienie.~~ **[Popr. 22]**

(20) Zobowiązanie dostawców usług hostingowych do zachowania usuniętych treści i związanych z nimi danych powinno być ustanowione do celów szczególnych i ograniczone w czasie do tego, co jest konieczne. Istnieje potrzeba rozszerzenia wymogu zachowania na powiązane dane w takim zakresie, w jakim jakiekolwiek tego rodzaju dane zostałyby utracone w wyniku usunięcia przedmiotowych treści. Powiązane dane mogą obejmować dane takie jak „dane abonenta", w ~~tym w~~ szczególności dane odnoszące się do tożsamości dostawcy treści oraz „dane dotyczące dostępu", w tym np. dane o dacie i czasie korzystania przez dostawcę treści lub o logowaniu do serwisu i wylogowaniu się z niego, wraz z adresem IP przydzielonym dostawcy treści przez dostawcę usług dostępu do internetu. **[Popr. 23]**

(21) Obowiązek zachowania treści do celów administracyjnego lub sądowego postępowania odwoławczego ***lub zaskarżenia*** jest konieczny i uzasadniony w celu zapewnienia skutecznych środków odwoławczych dostawcy treści, którego treści zostały usunięte lub do których dostęp został uniemożliwiony, jak również w celu przywrócenia tych treści w formie sprzed ich usunięcia, w zależności od wyniku procedury odwoławczej. Obowiązek zachowania treści do celów dochodzenia i ścigania jest uzasadniony i konieczny ze względu na wartość, jaką dany materiał mógłby wnieść w celu zakłócenia działalności terrorystycznej lub zapobieżenia jej. W przypadku gdy przedsiębiorstwa usuwają materiał lub uniemożliwiają dostęp do niego~~, w szczególności~~ za pomocą własnych ~~proaktywnych środków~~***środków szczególnych***, ~~i nie~~***jak najszybciej*** informują o tym ~~właściwego organu, ponieważ oceniają, że nie wchodzi to w zakres art. 13 ust. 4 niniejszego rozporządzenia, organy ścigania mogą nie~~***właściwe organy ścigania. Zachowanie treści do celów zapobiegania przestępstwom terrorystycznym***, ***ich wykrywania***, ***prowadzenia dochodzeń i ich ścigania jest również uzasadnione***. ***W tym celu treści o charakterze terrorystycznym i związane z nimi dane powinny*** być ~~świadome istnienia danych~~***przechowywane jedynie przez określony czas pozwalający organom ścigania na sprawdzenie ich*** treści ***i podjęcie decyzji, czy będą ona potrzebne do tych konkretnych czynności***. ***Termin ten nie powinien przekraczać sześciu miesięcy***. ~~Dlatego zachowanie treści~~ ***D***o celów zapobiegania przestępstwom terrorystycznym, ich wykrywania, prowadzenia dochodzeń i ~~ich~~ ścigania ~~jest również uzasadnione. Do~~ tych ~~celów~~***przestępstw*** wymagane zachowanie danych ogranicza się do danych, które mogą mieć związek z przestępstwami terrorystycznymi, a w związku z tym mogą przyczynić się do ścigania przestępstw terrorystycznych lub do zapobiegania poważnemu zagrożeniu bezpieczeństwa publicznego. **[Popr. 24]**

(22) W celu zapewnienia proporcjonalności okres zachowania powinien być ograniczony do sześciu miesięcy, aby dać dostawcom treści wystarczająco dużo czasu na rozpoczęcie procedury odwoławczej ~~oraz umożliwić~~***lub umożliwienie*** organom ścigania ~~dostęp~~***dostępu*** do odpowiednich danych na potrzeby dochodzenia i ścigania

przestępstw terrorystycznych. Okres ten może jednak zostać na wniosek organu prowadzącego postępowanie odwoławcze ***lub zaskarżenie*** przedłużony o niezbędny okres, w przypadku gdy wszczęte postępowanie odwoławcze nie zakończyło się w okresie sześciu miesięcy. Okres ten powinien ***również*** być wystarczający, aby organy ścigania mogły zachować niezbędne ~~dowody~~***materiały*** w związku z dochodzeniami ***i śledztwami***, a jednocześnie zapewnić równowagę z odpowiednimi prawami podstawowymi. **[Popr. 25]**

(23) Niniejsze rozporządzenie nie ma wpływu na gwarancje procesowe ani środki dochodzeniowe dotyczące dostępu do treści i powiązanych danych zachowanych do celów prowadzenia dochodzeń w sprawie przestępstw terrorystycznych i ich ścigania na podstawie prawa krajowego państw członkowskich oraz na podstawie prawodawstwa Unii.

(24) Przejrzystość polityki dostawców usług hostingowych wobec treści o charakterze terrorystycznym ma zasadnicze znaczenie dla zwiększenia ich odpowiedzialności wobec użytkowników oraz podniesienia zaufania obywateli do jednolitego rynku cyfrowego. ***Jedynie*** dostawcy usług hostingowych***, wobec których wydano nakazy usunięcia treści o charakterze terrorystycznym w danym roku,*** powinni ~~publikować roczne~~***być zobowiązani do opublikowania rocznego*** sprawozdania na temat przejrzystości ~~zawierające~~***zawierającego*** istotne informacje na temat działań podjętych w związku z wykrywaniem, identyfikacją i usuwaniem treści o charakterze terrorystycznym. **[Popr. 26]**

(24a) Organy właściwe do wydawania nakazu usunięcia powinny również publikować sprawozdania na temat przejrzystości zawierające informacje o liczbie wydanych nakazów usunięcia, liczbie odpowiedzi odmownych, liczbie zidentyfikowanych treści o charakterze terrorystycznym, które doprowadziły do wszczęcia dochodzenia i ścigania sprawców przestępstw terrorystycznych, oraz o liczbie przypadków treści, które zostały błędnie uznane za terrorystyczne. **[Popr. 27]**

(25) Procedury rozpatrywania skarg stanowią niezbędną gwarancję przeciwko błędnemu usuwaniu treści chronionych w ramach wolności wypowiedzi ***oraz wolności otrzymywania*** i ***przekazywania*** informacji ***i idei w otwartym i demokratycznym społeczeństwie***. W związku z tym dostawcy usług hostingowych powinni ustanowić przyjazne dla użytkownika mechanizmy rozpatrywania skarg oraz zapewnić, by skargi były rozpatrywane bezzwłocznie i przy pełnej przejrzystości wobec dostawcy treści. Wymóg, aby dostawca usług hostingowych przywrócił treści, w przypadku gdy zostały one błędnie usunięte, nie ma wpływu na możliwość egzekwowania przez dostawców usług hostingowych własnych warunków w innych przypadkach. **[Popr. 28]**

(26) Skuteczna ochrona prawna, zgodnie z art. 19 TUE i art. 47 Karty praw podstawowych Unii Europejskiej, wymaga, aby osoby były w stanie ustalić powody, dla których treści zamieszczone przez nie zostały usunięte lub dostęp do nich został uniemożliwiony. W tym celu dostawca usług hostingowych powinien udostępnić dostawcy treści istotne informacje ~~umożliwiające dostawcy treści zaskarżenie decyzji. Nie wymaga to jednak powiadomienia~~***, takie jak przyczyny usunięcia lub uniemożliwienia dostępu, a także informację o podstawie prawnej danego działania, umożliwiające*** dostawcy treści ***zaskarżenie decyzji***. W zależności od okoliczności dostawcy usług hostingowych mogą zastąpić treści uznane za treści o charakterze terrorystycznym komunikatem, że zostały usunięte lub dostęp do nich został uniemożliwiony zgodnie z niniejszym rozporządzeniem. ~~Na żądanie należy podać dalsze informacje na temat przyczyn oraz możliwości zaskarżenia decyzji przez dostawcę treści.~~ W przypadku gdy właściwe organy postanowią, że ze względu na bezpieczeństwo publiczne, w tym w kontekście dochodzenia, bezpośrednie powiadamianie dostawcy treści o usunięciu treści lub uniemożliwieniu dostępu do nich uznaje się za niewłaściwe lub przynoszące efekty odwrotne do zamierzonych, powinny poinformować o tym dostawcę usług hostingowych. **[Popr. 29]**

(27) W celu uniknięcia powielania działań i ingerencji w dochodzenia***, a także w celu ograniczenia do minimum kosztów ponoszonych przez danych dostawców usług,*** właściwe organy powinny przekazywać informacje, koordynować i współpracować ze sobą oraz, w stosownych przypadkach, z Europolem przy wydawaniu nakazów usunięcia ~~lub wysyłaniu zgłoszeń~~***skierowanych*** do dostawców usług hostingowych. Przy wdrażaniu przepisów niniejszego rozporządzenia wsparcie mógłby zapewnić Europol, zgodnie ze swoim obecnym mandatem oraz obowiązującymi ramami prawnymi. **[Popr. 30]**

(27a) Zgłoszenia dokonywane przez Europol stanowią skuteczny i szybki sposób informowania dostawców usług hostingowych o konkretnych treściach w ramach świadczonych przez nich usług. Taki mechanizm powiadamiania

dostawców usług hostingowych o informacjach, które mogą być uznawane za treści o charakterze terrorystycznym, w celu dobrowolnego rozważenia przez dostawcę zgodności z jego własnymi warunkami powinien pozostać dostępny jako uzupełnienie nakazów usunięcia. Ważne jest, aby dostawcy usług hostingowych współpracowali z Europolem, a także aby traktowali ocenę takich zgłoszeń przez Europol priorytetowo i przekazywali szybkie informacje zwrotne na temat podjętych działań. Ostateczna decyzja dotycząca tego, czy usunąć dane treści, ponieważ nie są one zgodne z warunkami dostawcy usług hostingowych, pozostaje w gestii danego dostawcy. Przy wdrażaniu niniejszego rozporządzenia mandat Europolu, określony w rozporządzeniu (UE) 2016/794 ([10]), pozostaje niezmieniony. **[Popr. 31]**

(28) W celu zapewnienia skutecznego i wystarczająco spójnego wdrożenia ~~proaktywnych środków~~***środków przez dostawców usług hostingowych*** właściwe organy w państwach członkowskich powinny współdziałać ze sobą w odniesieniu do rozmów ***prowadzonych*** z dostawcami usług hostingowych na temat ***nakazów usunięcia oraz*** określania, wdrażania i oceny ~~konkretnych~~ środków ~~proaktywnych~~***szczególnych***. Taka współpraca jest również konieczna w związku z przyjęciem przepisów dotyczących sankcji, a także wdrażania i egzekwowania sankcji. **[Popr. 32]**

(29) Ważne jest, aby właściwy organ w państwie członkowskim ~~odpowiedzialnym~~***, odpowiedzialny*** za nakładanie sankcji, był w pełni informowany o wydawaniu nakazów usunięcia ~~i zgłoszeń~~ oraz o późniejszej wymianie informacji między dostawcą usług hostingowych a ~~odpowiednim właściwym organem~~ ***odpowiednimi właściwymi organami w innych państwach członkowskich***. W tym celu państwa członkowskie powinny zapewnić odpowiednie ***i bezpieczne*** kanały komunikacji i mechanizmy umożliwiające szybką wymianę istotnych informacji. **[Popr. 33]**

(30) Aby ułatwić szybką wymianę informacji między właściwymi organami, jak również z dostawcami usług hostingowych, oraz aby uniknąć powielania działań, państwa członkowskie mogą korzystać z narzędzi opracowanych przez Europol, takich jak obecna aplikacja zarządzania zgłoszeniami podejrzanych treści w internecie (IRMa) lub narzędzia, które ją zastąpią.

(31) Ze względu na szczególnie poważne konsekwencje niektórych treści o charakterze terrorystycznym dostawcy usług hostingowych powinni niezwłocznie informować organy zainteresowanego państwa członkowskiego lub właściwe organy tam, gdzie mają miejsce prowadzenia działalności lub przedstawiciela prawnego, o wszelkich dowodach dotyczących przestępstw terrorystycznych, o których się dowiedzieli. W celu zapewnienia proporcjonalności obowiązek ten ogranicza się do przestępstw terrorystycznych zdefiniowanych w art. 3 ust. 1 dyrektywy (UE) 2017/541. Obowiązek informowania nie oznacza obowiązku aktywnego poszukiwania takich dowodów przez dostawców usług hostingowych. Zainteresowane państwo członkowskie jest państwem członkowskim, które ma jurysdykcję w zakresie dochodzenia i ścigania przestępstw terrorystycznych na podstawie dyrektywy (UE) 2017/541 w oparciu o obywatelstwo sprawcy lub potencjalnej ofiary przestępstwa lub o miejsce będące celem aktu terrorystycznego. W przypadku wątpliwości dostawcy usług hostingowych mogą przekazywać informacje Europolowi, który powinien postępować zgodnie ze swoim mandatem, w tym przekazywać informacje odpowiednim organom krajowym.

(32) Właściwe organy w państwach członkowskich powinny mieć możliwość korzystania z takich informacji w celu wdrożenia środków dochodzeniowych dostępnych na podstawie prawa państwa członkowskiego lub prawa Unii, w tym wystawiania europejskiego nakazu wydania dowodów na mocy rozporządzenia w sprawie w sprawie europejskiego nakazu wydania dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych i europejskiego nakazu zabezpieczenia dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych ([11]).

(33) Zarówno dostawcy usług hostingowych, jak i państwa członkowskie powinny ustanowić punkty kontaktowe w celu ułatwienia ~~sprawnego~~***szybkiego*** rozpatrywania nakazów usunięcia ~~i zgłoszeń~~. W odróżnieniu od przedstawiciela prawnego punkt kontaktowy służy celom operacyjnym. Punkt kontaktowy dostawcy usług hostingowych powinien obejmować wszelkie wyspecjalizowane środki umożliwiające elektroniczne wnoszenie nakazów usunięcia ~~i dokonywanie zgłoszeń~~ oraz środki techniczne i personalne umożliwiające ich ~~sprawne~~***szybkie*** przetwarzanie. Punkt kontaktowy dostawcy usług hostingowych nie musi znajdować się w Unii, a dostawca usług hostingowych może wyznaczyć istniejący punkt kontaktowy, pod warunkiem że ten punkt kontaktowy jest w stanie pełnić funkcje przewidziane w niniejszym rozporządzeniu. W celu zapewnienia usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do nich w ciągu jednej godziny od otrzymania nakazu usunięcia dostawcy usług hostingowych powinni zapewnić, by punkt kontaktowy był dostępny 24 godziny na dobę 7 dni w tygodniu. Informacje na temat punktu kontaktowego powinny zawierać informacje o języku, w którym można zwrócić się do

---

([10]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW (Dz.U. L 135 z 24.5.2016, s. 53).

([11]) COM(2018)0225 final.

punktu kontaktowego. Aby ułatwić komunikację między dostawcami usług hostingowych a właściwymi organami, dostawców usług hostingowych zachęca się do umożliwienia komunikacji w jednym z języków urzędowych Unii, w którym zredagowane są ich warunki. **[Popr. 34]**

(34) W przypadku braku ogólnego wymogu, by dostawcy usług zapewniali fizyczną obecność na terytorium Unii, należy zapewnić jasność co do tego, jurysdykcji którego państwa członkowskiego podlega dostawca usług hostingowych oferujący usługi w Unii. Co do zasady dostawca usług hostingowych podlega jurysdykcji państwa członkowskiego, w którym ma główne miejsce prowadzenia działalności lub w którym wyznaczył przedstawiciela prawnego. ~~Niemniej jednak, w przypadku gdy inne państwo członkowskie wydaje nakaz usunięcia, jego organy powinny mieć możliwość egzekwowania swoich nakazów poprzez zastosowanie środków przymusu o charakterze niekarnym, takich jak kary pieniężne.~~ Jeżeli chodzi o dostawców usług hostingowych, którzy nie mają miejsca prowadzenia działalności w Unii i nie wyznaczyli przedstawiciela prawnego, każde państwo członkowskie powinno mieć jednak możliwość nakładania sankcji, pod warunkiem przestrzegania zasady *ne bis in idem*. **[Popr. 35]**

(35) Dostawcy usług hostingowych, którzy nie mają miejsca prowadzenia działalności w Unii, powinni wyznaczyć na piśmie przedstawiciela prawnego w celu zapewnienia wypełniania i egzekwowania obowiązków na podstawie niniejszego rozporządzenia. ***Dostawcy usług hostingowych mogą korzystać z usług dotychczasowego przedstawiciela prawnego, pod warunkiem że jest on w stanie pełnić funkcje przewidziane w niniejszym rozporządzeniu.*** **[Popr. 36]**

(36) Przedstawiciel prawny powinien mieć uprawnienia do działania w imieniu dostawcy usług hostingowych.

(37) Do celów niniejszego rozporządzenia państwa członkowskie powinny wyznaczyć ~~właściwe organy. Wymóg wyznaczenia właściwych organów niekoniecznie wiąże się z koniecznością~~***jeden organ sądowy lub jeden organ administracyjny niezależny pod względem operacyjnym. Wymóg ten nie oznacza konieczności*** ustanowienia ~~nowych organów, lecz nowe organy mogą~~***nowego organu*** – ***organem tym może*** być ~~istniejącymi jednostkami odpowiedzialnymi~~***istniejąca jednostka odpowiedzialna*** za ~~funkcje określone~~ ***pełnienie funkcji określonych*** w niniejszym rozporządzeniu. Niniejsze rozporządzenie wymaga wyznaczenia ~~organów właściwych~~***organu właściwego*** do celów wydawania nakazów usunięcia, ~~dokonywania zgłoszeń oraz~~ nadzorowania ~~proaktywnych środków~~***środków szczególnych*** i nakładania sankcji. ~~To~~ Państwa członkowskie ~~decydują~~***powinny powiadomić Komisję*** o ~~tym, ile~~***wyznaczeniu właściwego organu na mocy niniejszego rozporządzenia***, ***a Komisja powinna opublikować w internecie wykaz właściwych*** organów ~~chcą wyznaczyć do tych zadań~~***poszczególnych państw członkowskich. Taki wykaz internetowy powinien być łatwo dostępny, aby ułatwić szybką weryfikację przez dostawców usług hostingowych autentyczności nakazów usunięcia***. **[Popr. 37]**

(38) Sankcje są niezbędne do zapewnienia skutecznego wywiązania się przez dostawców usług hostingowych z obowiązków wynikających z niniejszego rozporządzenia. Państwa członkowskie powinny przyjąć przepisy dotyczące sankcji, w tym, w stosownych przypadkach, wytyczne w sprawie nakładania kar pieniężnych. ~~Szczególnie surowe sankcje ustala się~~ ***Sankcje należy nałożyć*** w przypadku, gdy ~~dostawca~~ ***dostawcy*** usług hostingowych systematycznie ***i stale*** ~~nie usuwa treści o charakterze terrorystycznym lub systematycznie~~ nie ***dopełniają obowiązków wynikających z niniejszego rozporządzenia.*** ~~uniemożliwia dostępu do nich w ciągu jednej godziny od momentu otrzymania nakazu usunięcia. Nieprzestrzeganie przepisów w poszczególnych przypadkach może być karane przy jednoczesnym przestrzeganiu zasady *ne bis in idem* i zasady proporcjonalności oraz zapewnieniu, by sankcje takie uwzględniały systematyczne nieprawidłowości. Aby zagwarantować pewność prawa, w rozporządzeniu należy określić zakres, w jakim odpowiednie obowiązki mogą podlegać sankcjom.~~ Sankcje za nieprzestrzeganie art. 6 powinny być ~~przyjmowane wyłącznie w odniesieniu do obowiązków wynikających z wniosku o sprawozdanie na podstawie art. 6 ust. 2 lub z decyzji o narzuceniu dodatkowych proaktywnych środków na podstawie art. 6 ust. 4. Przy ustalaniu, czy nałożyć sankcje finansowe, należy odpowiednio uwzględnić zasoby finansowe dostawcy usług.~~ ***nakładane wyłącznie w odniesieniu do obowiązków wynikających z żądania wdrożenia dodatkowych środków szczególnych na podstawie art. 6 ust. 4. Przy ustalaniu, czy nałożyć sankcje finansowe, należy odpowiednio uwzględnić zasoby finansowe dostawcy usług. Ponadto właściwy organ powinien wziąć pod uwagę, czy dostawca usług hostingowych jest przedsiębiorstwem typu start-up albo przedsiębiorstwem z kategorii małych i średnich przedsiębiorstw, oraz powinien ustalić dla każdego przypadku, czy dostawca miał możliwość odpowiedniego zastosowania się do wydanego nakazu.*** Państwa członkowskie ~~zapewniają~~***powinny zapewnić***, aby sankcje nie zachęcały do usuwania treści, które nie są treściami o charakterze terrorystycznym. **[Popr. 38]**

(39) Stosowanie standardowych szablonów ułatwia współpracę i wymianę informacji między właściwymi organami i dostawcami usług, co umożliwia im szybszą i skuteczniejszą komunikację. Szczególnie ważne jest zapewnienie sprawnego działania po otrzymaniu nakazu usunięcia. Szablony obniżają koszty tłumaczenia i przyczyniają się do zapewnienia wysokiego standardu jakości. Formularze odpowiedzi powinny umożliwiać znormalizowaną wymianę informacji, co ma szczególne znaczenie w przypadku, gdy usługodawcy nie są w stanie spełnić wymogów.

Uwierzytelnione kanały przekazywania informacji mogą zagwarantować autentyczność nakazu usunięcia, w tym dokładność daty i godziny wysłania i otrzymania nakazu.

(40) W celu umożliwienia, w razie potrzeby, szybkiej zmiany treści szablonów, które mają być stosowane do celów niniejszego rozporządzenia, należy przekazać Komisji uprawnienia do przyjęcia aktów zgodnie z art. 290 Traktatu o funkcjonowaniu Unii Europejskiej w odniesieniu do zmiany załączników I, II i III do niniejszego rozporządzenia. Aby móc uwzględnić rozwój technologii i powiązanych z nią ram prawnych, Komisja powinna być również uprawniona do przyjmowania aktów delegowanych w celu uzupełnienia niniejszego rozporządzenia o wymogi techniczne dotyczące środków elektronicznych, które mają być stosowane przez właściwe organy do przekazywania nakazów usunięcia. Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na szczeblu ekspertów, oraz aby konsultacje te prowadzone były zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym w sprawie lepszego stanowienia prawa z dnia 13 kwietnia 2016 r. ([12]). W szczególności, aby zapewnić udział na równych zasadach Parlamentu Europejskiego i Rady w przygotowaniu aktów delegowanych, instytucje te otrzymują wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji mogą systematycznie brać udział w posiedzeniach grup eksperckich Komisji zajmujących się przygotowaniem aktów delegowanych.

(41) Państwa członkowskie powinny gromadzić informacje na temat wdrażania prawodawstwa***, w tym informacje o liczbie przypadków skutecznego wykrycia, zbadania i ścigania przestępstw terrorystycznych na podstawie niniejszego rozporządzenia***. Na potrzeby oceny prawodawstwa zostanie opracowany szczegółowy program monitorowania produktów, rezultatów i skutków niniejszego rozporządzenia. **[Popr. 39]**

(42) W oparciu o ustalenia i wnioski zawarte w sprawozdaniu z wdrażania oraz wyniki monitorowania Komisja powinna przeprowadzić ocenę niniejszego rozporządzenia ~~nie wcześniej niż trzy lata~~ po ***upływie roku od*** jego ~~wejściu w życie~~***wejścia w życie***. Ocena ta powinna opierać się na ~~pięciu~~***siedmiu*** kryteriach: skuteczności, ***konieczności, proporcjonalności,*** efektywności, adekwatności, spójności ~~i europejskiej~~***i unijnej*** wartości dodanej. W jej ramach ~~ocenione zostanie~~***należy ocenić*** funkcjonowanie poszczególnych środków operacyjnych i technicznych przewidzianych w rozporządzeniu, w tym skuteczność środków mających na celu poprawę wykrywania, identyfikacji i usuwania treści o charakterze terrorystycznym, skuteczność mechanizmów ochronnych oraz skutki dla potencjalnie ~~narażonych~~ ***zagrożonych*** praw ~~i interesów~~***podstawowych, w tym wpływ na wolność wypowiedzi oraz wolność otrzymywania i przesyłania informacji, wolność i pluralizm mediów, wolność działalności gospodarczej oraz prawa do prywatności i ochrony danych osobowych. Komisja powinna również ocenić wpływ na potencjalnie narażone interesy*** osób trzecich, ~~włącznie z przeglądem wymogu~~ ***w tym ponownie rozważyć wymóg*** informowania dostawców treści. **[Popr. 40]**

(43) Ponieważ cel niniejszego rozporządzenia, a mianowicie zapewnienie sprawnego funkcjonowania jednolitego rynku cyfrowego poprzez zapobieganie rozpowszechnianiu w internecie treści o charakterze terrorystycznym, nie może zostać osiągnięty w sposób wystarczający przez państwa członkowskie, natomiast ze względu na rozmiary i skutki ograniczenia możliwe jest jego lepsze osiągnięcie na poziomie Unii, może ona podjąć działania zgodne z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności, określoną w tym artykule, niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tego celu,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

SEKCJA I

PRZEPISY OGÓLNE

Artykuł 1

Przedmiot i zakres stosowania

1. W niniejszym rozporządzeniu ustanawia się ***ukierunkowane*** jednolite przepisy w celu ~~zapobiegania~~ ***zwalczania*** wykorzystywaniu usług hostingowych do ***publicznego*** rozpowszechniania w internecie treści o charakterze terrorystycznym. Ustanawia się w nim w szczególności: **[Popr. 41]**

([12]) Dz.U. L 123 z 12.5.2016, s. 1.

a) przepisy dotyczące ***rozsądnych i proporcjonalnych*** obowiązków w zakresie staranności, których mają przestrzegać dostawcy usług hostingowych w celu ~~zapobiegania rozpowszechnianiu~~***zwalczania publicznego rozpowszechniania*** treści o charakterze terrorystycznym za pośrednictwem ~~ich~~***świadczonych*** usług oraz zapewnienia, w razie potrzeby, szybkiego usuwania tych treści; **[Popr. 42]**

b) zestaw środków, które państwa członkowskie mają wprowadzić w celu identyfikowania treści o charakterze terrorystycznym, umożliwienia ich szybkiego usuwania przez dostawców usług hostingowych ***zgodnie z prawem Unii zapewniającym odpowiednie gwarancje wolności wypowiedzi oraz wolności otrzymywania*** i ***przesyłania informacji i idei w otwartym i demokratycznym społeczeństwie, a także w celu*** ułatwienia współpracy z właściwymi organami w innych państwach członkowskich, dostawcami usług hostingowych oraz, w stosownych przypadkach, z odpowiednimi organami Unii. **[Popr. 43]**

2. Niniejsze rozporządzenie stosuje się do dostawców usług hostingowych świadczących usługi ***dla społeczeństwa*** w Unii, niezależnie od ich głównego miejsca prowadzenia działalności. **[Popr. 44]**

2a. Niniejsze rozporządzenie nie ma zastosowania do treści rozpowszechnianych w celach edukacyjnych, artystycznych, dziennikarskich lub badawczych lub w celach zwiększenia świadomości na temat zwalczania działalności terrorystycznej ani do wyrażania polemicznych lub kontrowersyjnych poglądów w ramach debaty publicznej. **[Popr. 45]**

2b. Niniejsze rozporządzenie nie ma wpływu na obowiązek poszanowania praw, wolności i zasad, o których mowa w art. 6 Traktatu o Unii Europejskiej, i nie narusza podstawowych zasad prawa Unii i prawa krajowego odnoszących się do wolności słowa, wolności prasy oraz wolności i pluralizmu mediów. **[Popr. 46]**

2c. Niniejsze rozporządzenie nie narusza dyrektywy 2000/31/WE. **[Popr. 47]**

Artykuł 2

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

-1) „usługi społeczeństwa informacyjnego" oznaczają usługi, o których mowa w art. 2 lit. a) dyrektywy 2000/31/WE. **[Popr. 48]**

1) „dostawca usług hostingowych" oznacza dostawcę usług społeczeństwa informacyjnego polegających na przechowywaniu informacji dostarczonych przez dostawcę treści i na jego wniosek oraz na ***publicznym*** udostępnianiu przechowywanych informacji ~~osobom trzecim;~~***. Ma to zastosowanie wyłącznie do usług świadczonych na rzecz społeczeństwa w warstwie aplikacji. Dostawcy usług infrastruktury w chmurze oraz dostawcy usług w chmurze nie są uznawani za dostawców usług hostingowych. Nie ma to również zastosowania do usług łączności elektronicznej, o których mowa w dyrektywie (UE) 2018/1972***; **[Popr. 49]**

2) „dostawca treści" oznacza użytkownika, który dostarczył informacje, które są lub były przechowywane ***i publicznie udostępniane*** na wniosek użytkownika przez dostawcę usług hostingowych; **[Popr. 50]**

3) „oferowanie usług w Unii" oznacza: umożliwianie osobom prawnym lub fizycznym z jednego państwa członkowskiego lub większej ich liczby korzystania z usług dostawcy usług hostingowych, którego z danym państwem członkowskim lub danymi państwami członkowskimi łączy ścisły związek, taki jak:

a) posiadanie przez dostawcę usług hostingowych miejsca prowadzenia działalności w Unii;

b) znaczna liczba użytkowników w jednym państwie członkowskim lub większej ich liczbie;

c) ukierunkowanie prowadzonej działalności na jedno państwo członkowskie lub większą ich liczbę;

~~4) „przestępstwa terrorystyczne" oznaczają przestępstwa zdefiniowane w art. 3 ust. 1 dyrektywy (UE) 2017/541;~~ **[Popr. 51]**

Środa, 17 kwietnia 2019 r.

5) „treści o charakterze terrorystycznym" oznaczają ~~informacje~~ ***materiały*** należące do co najmniej jednej z następujących kategorii: **[Popr. 52]**

a) podżeganie do popełnienia ***jednego z*** przestępstw ~~terrorystycznych lub propagowanie popełniania tych przestępstw~~ ***wymienionych w art. 3 ust. 1 lit. a)–i) dyrektywy (UE) 2017/541***, w ~~tym~~***przypadku gdy takie postępowanie nakłania, bezpośrednio lub pośrednio, na przykład*** poprzez ~~ich gloryfikowanie, a przez to powodowanie ryzyka~~ ***gloryfikację aktów terrorystycznych***, ***do popełniania przestępstw terrorystycznych, co grozi tym, że dojdzie do umyślnego*** popełnienia ~~tych czynów:~~***jednego lub większej liczby takich przestępstw***; **[Popr. 53]**

b) ~~zachęcanie~~***nakłanianie innej osoby lub grupy osób*** do ~~przyczyniania~~ się do ***popełniania lub przyczynienia*** się do ***popełnienia jednego z*** przestępstw ~~terrorystycznych~~***wymienionych w art. 3 ust. 1 lit. a)–i) dyrektywy (UE) 2017/541, co grozi tym, że dojdzie do umyślnego popełnienia jednego lub większej liczby takich przestępstw***; **[Popr. 54]**

c) ~~propagowanie~~***nakłanianie innej osoby lub grupy osób do udziału w*** działalności grupy terrorystycznej, w ~~szczególności poprzez zachęcenie do udziału~~ ***tym przez dostarczanie informacji lub środków materialnych, lub przez finansowanie działalności tej grupy*** w ~~grupie terrorystycznej~~***jakikolwiek sposób*** w rozumieniu art. ~~2 ust. 3~~**4** dyrektywy (UE) 2017/541***, co grozi tym, że dojdzie*** ~~lub~~ do ~~jej wspierania~~***umyślnego popełnienia jednego lub większej liczby takich przestępstw***; **[Popr. 55]**

d) ~~instruowanie w zakresie~~***udzielanie instrukcji dotyczących wytwarzania lub stosowania materiałów wybuchowych, broni palnej lub innych rodzajów broni bądź trujących lub niebezpiecznych substancji, lub innych szczególnych*** metod lub technik ~~do celów popełniania~~***w celu popełnienia lub przyczynienia się*** do ***popełnienia jednego z*** przestępstw ~~terrorystycznych:~~***terrorystycznych wymienionych w art. 3 ust. 1 lit. a)–i) dyrektywy (UE) 2017/541;*** **[Popr. 56]**

da) przedstawianie popełniania jednego lub większej liczby przestępstw wymienionych w art. 3 ust. 1 lit. a)–i) dyrektywy (UE) 2017/541, co grozi tym, że dojdzie do umyślnego popełnienia jednego lub większej liczby takich przestępstw; **[Popr. 57]**

6) „rozpowszechnianie treści o charakterze terrorystycznym" oznacza udostępnianie treści o charakterze terrorystycznym ~~osobom trzecim~~***ogółowi społeczeństwa*** za pośrednictwem usług świadczonych przez dostawców usług hostingowych; **[Popr. 58]**

7) „warunki" oznaczają wszystkie warunki i klauzule, niezależnie od ich nazwy lub formy, które regulują stosunek umowny między dostawcą usług hostingowych a ich użytkownikami;

~~8) „zgłoszenie" oznacza zawiadomienie skierowane przez właściwy organ lub, w stosownych przypadkach, odpowiedni organ Unii do dostawcy usług hostingowych, dotyczące informacji, które można uznać za treści o charakterze terrorystycznym, celem dobrowolnego zbadania przez danego dostawcę zgodności tych informacji z jego własnymi warunkami mającymi na celu zapobieganie rozpowszechnianiu treści o charakterze terrorystycznym;~~ **[Popr. 59]**

9) „główne miejsce prowadzenia działalności" oznacza siedzibę główną lub siedzibę statutową, w ramach której wykonywane są główne funkcje finansowe i sprawowany jest nadzór operacyjny.

9a) „właściwy organ" oznacza jeden organ sądowy lub niezależny organ administracyjny wyznaczony w państwie członkowskim; **[Popr. 60]**

Środa, 17 kwietnia 2019 r.

SEKCJA II

ŚRODKI W CELU ZAPOBIEGANIA ROZPOWSZECHNIANIU W INTERNECIE TREŚCI O CHARAKTERZE TERRORYSTYCZNYM

Artykuł 3

Obowiązki w zakresie staranności

1. Dostawcy usług hostingowych podejmują ~~odpowiednie, rozsądne i proporcjonalne~~ działania zgodnie z niniejszym rozporządzeniem ~~przeciwko rozpowszechnianiu w internecie treści o charakterze terrorystycznym oraz~~ w celu ochrony użytkowników przed treściami o charakterze terrorystycznym. Działają przy tym ~~w sposób staranny~~***z zachowaniem należytej staranności, w sposób*** proporcjonalny i niedyskryminacyjny oraz z należytym uwzględnieniem ***we wszystkich okolicznościach*** praw podstawowych użytkowników~~, a także~~ uwzględniają podstawowe znaczenie wolności wypowiedzi ***oraz wolności otrzymywania*** i ***przekazywania*** informacji ***i idei*** w otwartym i demokratycznym społeczeństwie***, tak aby uniknąć usuwania treści, które nie mają charakteru terrorystycznego***. **[Popr. 61]**

1a. Obowiązki w zakresie staranności nie powinny stanowić ogólnego obowiązku monitorowania przez dostawców usług hostingowych informacji, które przekazują lub przechowują, ani ogólnego obowiązku aktywnego poszukiwania faktów lub okoliczności wskazujących na działalność niezgodną z prawem. **[Popr. 62]**

~~2. Dostawcy usług hostingowych uwzględniają w swoich warunkach i stosują przepisy zapobiegające rozpowszechnianiu treści o charakterze terrorystycznym.~~ **[Popr. 63]**

2a. W przypadku gdy dostawcy usług hostingowych dowiedzą się o treściach o charakterze terrorystycznym w ramach świadczonych usług bądź staną się świadomi takich treści, informują o tych treściach właściwe organy i szybko te treści usuwają. **[Popr. 64]**

2b. Dostawcy usług hostingowych, którzy spełniają kryteria definicji dostawców platform udostępniania plików wideo przewidzianej w dyrektywie (UE) 2018/1808, przyjmują odpowiednie środki służące zwalczaniu rozpowszechniania treści o charakterze terrorystycznym zgodnie z art. 28b ust. 1 lit. c) i ust. 3 dyrektywy (UE) 2018/1808. **[Popr. 65]**

Artykuł 4

Nakazy usunięcia

1. Właściwy organ ~~jest uprawniony do wydania decyzji zobowiązującej dostawcę~~***państwa członkowskiego, w którym dostawca*** usług hostingowych ***ma główną siedzibę, jest uprawniony*** do ***wydania temu dostawcy nakazu*** usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do nich ***we wszystkich państwach członkowskich***. **[Popr. 66]**

1a. Właściwy organ państwa członkowskiego, w którym dostawca usług hostingowych nie posiada głównej siedziby lub nie ma przedstawiciela prawnego, może żądać uniemożliwienia dostępu do treści o charakterze terrorystycznym i wyegzekwować ten wymóg na swoim terytorium. **[Popr. 67]**

1b. Jeżeli odnośny właściwy organ nie nakazał uprzednio dostawcy usług hostingowych usunięcia treści, powinien skontaktować się z tym dostawcą, przekazując mu informacje na temat procedur i obowiązujących terminów co najmniej 12 godzin przed wydaniem nakazu usunięcia. **[Popr. 68]**

2. Dostawcy usług hostingowych usuwają treści o charakterze terrorystycznym lub uniemożliwiają dostęp do nich ***jak najszybciej i*** w ciągu ~~jednej~~ godziny od ~~momentu~~ otrzymania nakazu usunięcia. **[Popr. 69]**

3. Nakazy usunięcia zawierają następujące elementy zgodnie z szablonem określonym w załączniku I:

a) wskazanie ***za pomocą podpisu elektronicznego*** właściwego organu wydającego nakaz usunięcia i potwierdzenie autentyczności nakazu usunięcia przez właściwy organ; **[Popr. 70]**

Środa, 17 kwietnia 2019 r.

b) ~~uzasadnienie~~***szczegółowe uzasadnienie***, dlaczego ~~przedmiotowe~~***dane*** treści uznaje się za treści o charakterze terrorystycznym, ~~przynajmniej poprzez~~***oraz konkretne*** odniesienie do kategorii treści o charakterze terrorystycznym wymienionych w art. 2 pkt 5; **[Popr. 71]**

c) ***dokładny*** ujednolicony format adresowania zasobów (URL) oraz, w razie potrzeby, dodatkowe informacje umożliwiające identyfikację zgłaszanych treści; **[Popr. 72]**

d) odesłanie do niniejszego rozporządzenia jako podstawy prawnej nakazu usunięcia;

e) znacznik daty i czasu wystawienia;

f) ***łatwo zrozumiałe*** informacje na temat środków odwoławczych ~~dostępnych dla~~***przysługujących*** dostawcy usług hostingowych i dostawcy treści***, w tym informacje o środkach odwoławczych do właściwego organu, a także wniesienia odwołania do sądu, wraz z terminami na wniesienie takich odwołań***; **[Popr. 73]**

g) ~~w stosownych przypadkach~~ ***gdy jest to konieczne i proporcjonalne*** – decyzję o nieujawnianiu informacji o usunięciu treści o charakterze terrorystycznym lub uniemożliwieniu dostępu do nich, o której mowa w art. 11. **[Popr. 74]**

~~4. Na wniosek dostawcy usług hostingowych lub dostawcy treści właściwy organ przedstawia szczegółowe uzasadnienie bez uszczerbku dla obowiązku dostawcy usług hostingowych polegającego na wykonaniu nakazu usunięcia w terminie określonym w ust. 2.~~ **[Popr. 75]**

5. ~~Właściwe organy kierują~~***Właściwy organ kieruje*** nakazy usunięcia do głównego miejsca prowadzenia działalności dostawcy usług hostingowych lub do przedstawiciela prawnego wyznaczonego przez dostawcę usług hostingowych na podstawie art. 16 i ~~przekazują~~ ***przekazuje*** je punktowi kontaktowemu, o którym mowa w art. 14 ust. 1. Nakazy te są wysyłane za pomocą środków elektronicznych zdolnych do sporządzenia pisemnego rejestru na warunkach, które umożliwiają ustalenie autentyczności nadawcy oraz podanie dokładnej daty i czasu wysłania i otrzymania nakazu. **[Popr. 76]**

6. Dostawcy usług hostingowych ~~potwierdzają odbiór i~~ bez zbędnej zwłoki informują właściwy organ o usunięciu treści o charakterze terrorystycznym lub uniemożliwieniu dostępu do nich, wskazując w szczególności czas podjęcia działań, z wykorzystaniem szablonu określonego w załączniku II. **[Popr. 77]**

7. Jeżeli dostawca usług hostingowych nie jest w stanie wykonać nakazu usunięcia ze względu na siłę wyższą lub faktyczną niemożliwość, których nie można przypisać dostawcy usług hostingowych, ***lub ze względów technicznych lub operacyjnych,*** informuje o tym bez zbędnej zwłoki właściwy organ, wyjaśniając przyczyny, z wykorzystaniem szablonu określonego w załączniku III. Termin określony w ust. 2 ma zastosowanie od momentu, gdy przywołane przyczyny ustąpią. **[Popr. 78]**

8. ~~Jeżeli dostawca~~***Dostawca*** usług hostingowych ~~nie jest w stanie wykonać~~***może odmówić wykonania*** nakazu usunięcia, ~~ponieważ~~***jeżeli*** nakaz ~~usunięcia~~***ten*** zawiera oczywiste błędy lub nie zawiera ~~informacji~~ wystarczających ~~do wykonania nakazu,~~ ***informacji.*** Informuje ***on*** o tym bez zbędnej zwłoki właściwy organ, zwracając się o niezbędne wyjaśnienia, z wykorzystaniem szablonu określonego w załączniku III. Termin określony w ust. 2 ma zastosowanie od momentu, gdy wyjaśnienia zostaną przedstawione. **[Popr. 79]**

9. Właściwy organ, który wydał nakaz usunięcia, powiadamia właściwy organ, który nadzoruje wdrażanie ~~proaktywnych~~ środków ***szczególnych***, o których mowa w art. 17 ust. 1 lit. c), kiedy nakaz usunięcia stanie się prawomocny. Nakaz usunięcia staje się prawomocny, jeżeli nie złożono od niego odwołania w terminie zgodnym z mającym zastosowanie prawem krajowym lub jeżeli został on utrzymany w mocy w następstwie odwołania. **[Popr. 80]**

Artykuł 4a

Procedura konsultacji w przypadku nakazów usunięcia

1. Jednocześnie ze zgodnym z art. 4 ust. 5 przekazaniem dostawcom usług hostingowych nakazu usunięcia, właściwy organ sądowy, o którym mowa w art. 4 ust. 1 lit. a, przekazuje kopię nakazu usunięcia właściwemu organowi, o którym mowa w art. 17 ust. 1 lit. a), państwa członkowskiego, w którym znajduje się główne miejsce prowadzenia działalności dostawcy usług hostingowych.

2. W przypadkach gdy właściwy organ państwa członkowskiego, w którym znajduje się główne miejsce prowadzenia działalności dostawcy usług hostingowych, ma uzasadnione podstawy, by przypuszczać, że przedmiotowy nakaz usunięcia może naruszać podstawowe interesy tego państwa członkowskiego, informuje o tym właściwy organ wydający. Organ wydający bierze te okoliczności pod uwagę i w stosownych przypadkach wycofuje lub dostosowuje nakaz usunięcia. **[Popr. 81]**

Artykuł 4b

Procedura współpracy w celu wydania dodatkowego nakazu usunięcia

1. Jeżeli właściwy organ wydał nakaz wydalenia zgodnie z art. 4 ust. 1a, organ ten może skontaktować się z właściwym organem państwa członkowskiego, w którym dostawca usług hostingowych ma siedzibę główną, w celu złożenia wniosku, aby właściwy organ państwa członkowskiego również wydał nakaz wydalenia zgodnie z art. 4 ust. 1.

2. Właściwy organ w państwie członkowskim, w którym znajduje się główna siedziba dostawcy usług hostingowych, wydaje nakaz wydalenia albo odmawia jego wydania możliwe jak najszybciej, ale nie później niż jedną godzinę od otrzymania wniosku zgodnie z ust. 1, i informuje o swojej decyzji właściwy organ, który wydał pierwszy nakaz.

3. W przypadku gdy właściwy organ w państwie członkowskim, w którym znajduje się główna siedziba, potrzebuje więcej niż jednej godziny na dokonanie własnej oceny treści, przesyła on do danego dostawcy usług hostingowych wniosek o tymczasowe wyłączenie dostępu do treści przez okres do 24 godzin, w którym to okresie właściwy organ dokonuje oceny i wysyła polecenie wycofania lub wycofuje wniosek o wyłączenie dostępu. **[Popr. 82]**

~~Artykuł 5~~

~~Zgłoszenia~~

~~1. Właściwy organ lub odpowiedni organ Unii mogą skierować zgłoszenie do dostawcy usług hostingowych.~~

~~2. Dostawcy usług hostingowych wprowadzają środki operacyjne i techniczne ułatwiające szybką ocenę treści, które zostały zgłoszone przez właściwe organy oraz, w stosownych przypadkach, odpowiednie organy Unii do dobrowolnego rozważenia.~~

~~3. Zgłoszenie jest skierowane do głównego miejsca prowadzenia działalności dostawcy usług hostingowych lub do przedstawiciela prawnego wyznaczonego przez dostawcę usług na podstawie art. 16 i przekazywane punktowi kontaktowemu, o którym mowa w art. 14 ust. 1. Zgłoszenia takie są wysyłane za pomocą środków elektronicznych.~~

~~4. Zgłoszenie zawiera wystarczająco szczegółowe informacje, w tym powody, dla których treści uważa się za treści o charakterze terrorystycznym, URL oraz, w razie potrzeby, dodatkowe informacje umożliwiające identyfikację zgłaszanych treści o charakterze terrorystycznym.~~

~~5. Dostawca usług hostingowych ocenia, w trybie priorytetowym, treści zidentyfikowane w zgłoszeniu w świetle swoich własnych warunków i podejmuje decyzję, czy usunąć te treści lub uniemożliwić dostęp do nich.~~

Środa, 17 kwietnia 2019 r.

~~6. Dostawca usług hostingowych niezwłocznie informuje właściwy organ lub właściwy organ unijny o wyniku oceny oraz o tym, kiedy podjęto wszelkie działania w wyniku zgłoszenia.~~

~~7. W przypadku gdy dostawca usług hostingowych uważa, że zgłoszenie nie zawiera informacji wystarczających do dokonania oceny zgłoszonych treści, niezwłocznie informuje o tym właściwe organy lub właściwy organ Unii, określając, jakie dalsze informacje lub wyjaśnienia są wymagane.~~ **[Popr. 83]**

Artykuł 6

~~*Proaktywne*~~***Szczególne*** środki **[Popr. 84]**

1. ~~W stosownych przypadkach~~***Z zastrzeżeniem dyrektywy (UE) 2018/1808 i dyrektywy 2000/31/WE*** dostawcy usług hostingowych ~~wprowadzają proaktywne~~***mogą wprowadzić konkretne*** środki w celu ochrony swoich usług przed ***publicznym*** rozpowszechnianiem treści o charakterze terrorystycznym. Środki te są skuteczne***, ukierunkowane*** i proporcjonalne ~~oraz uwzględniają zagrożenie~~***do zagrożenia, ze szczególnym uwzględnieniem ryzyka*** i ~~poziom~~***poziomu*** narażenia na treści o charakterze terrorystycznym~~, prawa podstawowe~~ ***oraz praw podstawowych*** użytkowników ~~oraz podstawowe znaczenie~~***, a także podstawowego znaczenia*** wolności wypowiedzi ***oraz otrzymywania*** i ***przekazywania*** informacji ***i praw do prywatności i idei*** w otwartym i demokratycznym społeczeństwie. **[Popr. 85]**

~~2. Właściwy organ, o którym mowa w art. 17 ust. 1 lit. c), przypadku gdy został powiadomiony zgodnie z art. 4 ust. 9, zwraca się z wnioskiem do dostawcy usług hostingowych o przedłożenie w terminie trzech miesięcy od otrzymania wniosku, a następnie co najmniej raz w roku, sprawozdania na temat szczególnych proaktywnych środków, które wprowadził, w tym za pomocą zautomatyzowanych narzędzi, w celu:~~

~~a) zapobiegania ponownemu zamieszczaniu treści, które wcześniej zostały usunięte lub do których dostęp został uniemożliwiony, ponieważ uznaje się je za treści o charakterze terrorystycznym;~~

~~b) wykrywania, identyfikacji i szybkiego usuwania treści o charakterze terrorystycznym lub uniemożliwiania dostępu do nich.~~

~~Wniosek taki wysyła się do głównego miejsca prowadzenia działalności dostawcy usług hostingowych lub do przedstawiciela prawnego wyznaczonego przez dostawcę usług.~~

~~Sprawozdania zawierają wszelkie istotne informacje umożliwiające właściwemu organowi, o którym mowa w art. 17 ust. 1 lit. c), ocenę skuteczności i proporcjonalności proaktywnych środków, w tym ocenę funkcjonowania wszelkich wykorzystywanych zautomatyzowanych narzędzi oraz stosowanych mechanizmów weryfikacji i nadzoru przez człowieka.~~ **[Popr. 86]**

~~3. W przypadku gdy właściwy organ, o którym mowa w art. 17 ust. 1 lit. c), uzna, że proaktywne środki wprowadzone i ujęte w sprawozdaniu zgodnie z ust. 2 są niewystarczające do ograniczenia ryzyka i poziomu narażenia oraz do zarządzania tym ryzykiem i poziomem narażenia, może zażądać od dostawcy usług hostingowych wprowadzenia dodatkowych szczególnych proaktywnych środków. W tym celu dostawca usług hostingowych współpracuje z właściwym organem, o którym mowa w art. 17 ust. 1 lit. c), w celu określenia szczególnych środków, jakie dostawca usług hostingowych ma wdrożyć, ustanowienia kluczowych celów i poziomów odniesienia, a także harmonogramu ich wdrożenia.~~ **[Popr. 87]**

4. ~~Jeżeli w ciągu trzech miesięcy od zwrócenia się z wnioskiem na podstawie ust. 3 nie można osiągnąć porozumienia,~~ ***Po ustaleniu, że dostawca usług hostingowych otrzymał znaczną liczbę nakazów usunięcia,*** właściwy organ, o którym mowa w art. 17 ust. 1 lit. c), może ~~wydać decyzję o narzuceniu szczególnych dodatkowych niezbędnych i proporcjonalnych proaktywnych~~***wystąpić z wnioskiem*** o ***podjęcie niezbędnych, proporcjonalnych*** i ***skutecznych dodatkowych*** środków ***szczególnych, które dostawca usług hostingowych będzie musiał wdrożyć***. ***Właściwy organ nie nakłada ogólnego obowiązku monitorowania ani wykorzystania zautomatyzowanych narzędzi.*** ~~W decyzji~~***We wniosku tym*** uwzględnia się w szczególności ***techniczną wykonalność środków, wielkość i*** zdolność ekonomiczną dostawcy usług hostingowych oraz wpływ takich środków na prawa podstawowe użytkowników, a także podstawowe znaczenie wolności wypowiedzi ***oraz otrzymywania*** i ***przekazywania*** informacji ***i idei w otwartym i demokratycznym społeczeństwie***. ~~Decyzję taką~~***Wniosek taki*** wysyła się do głównego miejsca prowadzenia działalności dostawcy usług hostingowych lub do przedstawiciela prawnego wyznaczonego przez dostawcę usług. Dostawca usług hostingowych regularnie składa sprawozdania z wdrażania takich środków określonych przez właściwy organ, o którym mowa w art. 17 ust. 1 lit. c). **[Popr. 88]**

5. Dostawca usług hostingowych może w dowolnym momencie zwrócić się do właściwego organu, o którym mowa w art. 17 ust. 1 lit. c), o przegląd oraz, w stosownych przypadkach, o cofnięcie wniosku ~~lub decyzji odpowiednio~~ na podstawie ust. ~~2, 3 i~~ 4. Właściwy organ wydaje uzasadnioną decyzję w rozsądnym terminie od otrzymania wniosku od dostawcy usług hostingowych. **[Popr. 89]**

Artykuł 7

Zachowanie treści i związanych z nimi danych

1. Dostawcy usług hostingowych zachowują treści o charakterze terrorystycznym, które zostały usunięte lub do których dostęp został uniemożliwiony w wyniku nakazu usunięcia~~, zgłoszenia~~ lub w wyniku ~~proaktywnych~~***szczególnych*** środków na podstawie art. 4, ~~5~~ i 6, oraz związane z nimi dane, które zostały usunięte w wyniku usunięcia treści o charakterze terrorystycznym, które są konieczne do: **[Popr. 90]**

a) administracyjnego lub sądowego postępowania odwoławczego***, kontroli sądowej lub środków zaskarżenia***, **[Popr. 91]**

b) zapobiegania przestępstwom terrorystycznym, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania ***przez organy ścigania***. **[Popr. 92]**

2. Treści o charakterze terrorystycznym i związane z nimi dane, o których mowa w ust. 1 ***lit. a)***, zachowuje się przez sześć miesięcy ***i usuwa po upływie tego okresu***. ***Nielegalne*** treści o charakterze terrorystycznym są, na wniosek właściwego organu lub sądu, zachowywane przez ***konkretny*** dłuższy okres ~~oraz~~ ***tylko jeżeli jest to konieczne i tylko*** tak długo, jak jest to konieczne do celów toczącego się postępowania administracyjnego lub sądowego, ***kontroli sądowej lub środków zaskarżenia,*** o ~~którym~~ ***których*** mowa w ust. 1 lit. a). ***Dostawcy usług hostingowych przechowują treści terrorystyczne i powiązane z nimi dane, o których mowa w ust. 1 lit. b), dopóki organ ścigania nie odpowie na powiadomienie dokonane przez dostawcę usług hostingowych zgodnie z art. 13 ust. 4, jednak nie później niż w terminie sześciu miesięcy.*** **[Popr. 93]**

3. Dostawcy usług hostingowych zapewniają, aby treści o charakterze terrorystycznym i związane z nimi dane zachowane na podstawie ust. 1 i 2 podlegały odpowiednim gwarancjom technicznym i organizacyjnym.

Wspomniane gwarancje techniczne i organizacyjne zapewniają, by dostęp do zachowanych treści o charakterze terrorystycznym i związanych z nimi danych oraz ich przetwarzanie odbywały się wyłącznie do celów, o których mowa w ust. 1, i zapewniają wysoki poziom ochrony odnośnych danych osobowych. W razie potrzeby dostawcy usług hostingowych dokonują przeglądu i aktualizacji tych gwarancji.

SEKCJA III

GWARANCJE I ODPOWIEDZIALNOŚĆ

Artykuł 8

Obowiązki ***dostawców usług hostingowych*** w zakresie przejrzystości **[Popr. 94]**

1. ~~Dostawcy~~***W stosownych przypadkach dostawcy*** usług hostingowych ***jasno*** określają w swoich warunkach własną politykę zapobiegania rozpowszechnianiu treści o charakterze terrorystycznym, w tym, w stosownych przypadkach, rzeczowe wyjaśnienie funkcjonowania proaktywnych ~~środków, w tym wykorzystania zautomatyzowanych narzędzi~~ ***szczególnych środków***. **[Popr. 95]**

2. Dostawcy usług hostingowych ~~publikują~~***, wobec których w danym roku wystawiono nakaz usunięcia, udostępniają publicznie*** roczne ~~sprawozdania~~***sprawozdanie*** na temat przejrzystości w odniesieniu do podejmowanych działań wymierzonych przeciwko rozpowszechnianiu treści o charakterze terrorystycznym. **[Popr. 96]**

3. Sprawozdania na temat przejrzystości zawierają co najmniej następujące informacje:

a) informacje na temat środków wprowadzonych przez dostawcę usług hostingowych w związku z wykrywaniem, identyfikacją i usuwaniem treści o charakterze terrorystycznym;

Środa, 17 kwietnia 2019 r.

b) informacje na temat środków wprowadzonych przez dostawcę usług hostingowych w celu zapobiegania ponownemu zamieszczaniu treści, które wcześniej zostały usunięte lub do których dostęp został uniemożliwiony, ponieważ uznaje się je za treści o charakterze terrorystycznym***, szczególnie w przypadkach, w których zastosowano technologię zautomatyzowaną***; **[Popr. 97]**

c) liczbę przypadków usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do takich treści w wyniku odpowiednio nakazów usunięcia~~, zgłoszeń~~ lub ~~proaktywnych~~ ***szczególnych*** środków***, oraz liczbę nakazów, w przypadku których treść nie została usunięta zgodnie z art. 4 ust. 7 i 8 wraz z powodami odmowy.***; **[Popr. 98]**

d) ~~przegląd~~***liczbę*** i wyniki procedur rozpatrywania skarg ***i skarg o kontrolę sądową, w tym liczba przypadków, w odniesieniu do których ustalono, że treści zostały błędnie zidentyfikowane jako treści o charakterze terrorystycznym***. **[Popr. 99]**

Artykuł 8a

Obowiązki właściwych organów w zakresie przejrzystości

1. Właściwe organy publikują roczne sprawozdania dotyczące przejrzystości zawierające przynajmniej następujące informacje:

a) liczba wydanych nakazów usunięcia, liczba usunięć i liczba odrzuconych lub zignorowanych nakazów usunięcia;

b) liczba zidentyfikowanych treści terrorystycznych, które doprowadziły do dochodzenia i ścigania przestępstw oraz liczba przypadków treści błędnie uznanych za terrorystyczne;

c) opis środków wymaganych przez właściwe organy zgodnie z art. 6 ust. 4. **[Popr. 100]**

Artykuł 9

Gwarancje dotyczące stosowania i wdrażania ~~proaktywnych~~***szczególnych*** środków **[Popr. 101]**

1. Jeżeli dostawcy usług hostingowych korzystają ~~na podstawie niniejszego rozporządzenia~~ ze zautomatyzowanych mechanizmów w odniesieniu do przechowywanych przez siebie treści, dostarczają oni skutecznych i odpowiednich gwarancji zapewniających, by decyzje podejmowane w sprawie takich treści, zwłaszcza decyzje o usunięciu treści uznanych za treści o charakterze terrorystycznym lub o uniemożliwieniu dostępu do nich, były precyzyjne i uzasadnione. **[Popr. 102]**

2. Takie gwarancje obejmują przede wszystkim nadzór i weryfikację przez człowieka ~~w przypadkach, gdy jest to właściwe, oraz zawsze, gdy~~ ***właściwości decyzji dotyczącej usunięcia treści lub odmowy dostępu*** do ~~ustalenia, czy treści należy uznać za treści o charakterze terrorystycznym, czy też nie, wymagana jest szczegółowa ocena danego kontekstu~~ ***treści, w szczególności w odniesieniu do prawa do wolności wypowiedzi oraz wolności otrzymywania i przekazywania informacji i idei w otwartym i demokratycznym społeczeństwie***. **[Popr. 103]**

Artykuł 9a

Skuteczne środki ochrony prawnej

1. Dostawcy treści, których treści zostały usunięte lub do których dostęp został uniemożliwiony w wyniku nakazu usunięcia, oraz dostawcy usług hostingowych, którzy otrzymali nakaz usunięcia, mają prawo do skutecznego środka odwoławczego. Państwa członkowskie wprowadzają skuteczne procedury korzystania z tego prawa. **[Popr. 104]**

Artykuł 10

Mechanizmy rozpatrywania skarg

1. Dostawcy usług hostingowych ustanawiają skuteczne i dostępne mechanizmy umożliwiające dostawcom treści, których treści zostały usunięte lub dostęp do nich uniemożliwiony w wyniku ~~zgłoszenia na podstawie art. 5 lub proaktywnych~~***szczególnych*** środków na podstawie art. 6, złożenie skargi na działanie dostawcy usług hostingowych z żądaniem przywrócenia treści. **[Popr. 105]**

2. Dostawcy usług hostingowych niezwłocznie rozpatrują każdą skargę, którą otrzymują, i bez zbędnej zwłoki przywracają treści, w przypadku gdy usunięcie lub uniemożliwienie dostępu było nieuzasadnione. Informują oni składającego skargę o wyniku rozpatrzenia skargi ***w terminie dwóch tygodni od jej otrzymania, z podaniem precyzyjnego wyjaśnienia w przypadkach, w których dostawcy usług hostingowych zdecydują o nieprzywracaniu treści. Przywrócenie treści nie wyklucza możliwości skorzystania z innych środków sądowych w związku z decyzją dostawcy usług hostingowych lub właściwego organu***. **[Popr. 106]**

Artykuł 11

Informacje dla dostawców treści

1. W przypadku gdy dostawcy usług hostingowych ~~usuną~~***usuwają*** treści o charakterze terrorystycznym lub uniemożliwią dostęp do nich, udostępniają oni dostawcy treści ***zrozumiałe i zwięzłe*** informacje na temat takiego usunięcia lub ~~uniemożliwiania~~***uniemożliwienia*** dostępu do treści o charakterze terrorystycznym ***oraz możliwości odwołania się od decyzji, a także na wniosek dostawcy dostarczają mu kopię nakazu usunięcia wystawionego zgodnie z art. 4***. **[Popr. 107]**

~~2. Na wniosek dostawcy treści dostawca usług hostingowych informuje dostawcę treści o przyczynach usunięcia lub uniemożliwienia dostępu oraz o możliwościach zaskarżenia tej decyzji.~~ **[Popr. 108]**

3. Obowiązek na podstawie ust. 1 ~~i 2~~ nie ma zastosowania, jeżeli właściwy organ zdecyduje, ***na podstawie obiektywnych dowodów i z uwzględnieniem proporcjonalności i konieczności takiej decyzji,*** że nie powinno się ujawniać informacji ze względów bezpieczeństwa publicznego, takich jak zapobieganie przestępstwom terrorystycznym, prowadzenie dochodzeń w ich sprawie, wykrywanie i ściganie takich przestępstw, tak długo, jak to konieczne, ale nie dłużej niż [cztery] tygodnie od tej decyzji. W takim przypadku dostawca usług hostingowych nie ujawnia żadnych informacji dotyczących usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do nich. **[Popr. 109]**

SEKCJA IV

WSPÓŁPRACA MIĘDZY WŁAŚCIWYMI ORGANAMI, ORGANAMI UNII I DOSTAWCAMI USŁUG HOSTINGOWYCH

Artykuł 12

Zdolności właściwych organów

Państwa członkowskie zapewniają, aby ich właściwe organy dysponowały niezbędnymi zdolnościami i wystarczającymi zasobami, aby osiągnąć cele i wypełnić swoje obowiązki na podstawie niniejszego rozporządzenia***, przy silnych gwarancjach niezależności***. **[Popr. 110]**

Artykuł 13

Współpraca między dostawcami usług hostingowych, właściwymi organami oraz, w stosownych przypadkach, ~~odpowiednimi~~ **właściwymi** organami Unii **[Popr. 111]**

1. Właściwe organy w państwach członkowskich przekazują informacje, koordynują i współpracują ze sobą oraz, w stosownych przypadkach, z ~~odpowiednimi organami Unii takimi jak Europol~~ ***Europolem*** w odniesieniu do nakazów usunięcia ~~i zgłoszeń~~ w celu uniknięcia powielania działań, a także w celu poprawy koordynacji i uniknięcia ingerencji w dochodzenia prowadzone w różnych państwach członkowskich. **[Popr. 112]**

Środa, 17 kwietnia 2019 r.

2. Właściwe organy w państwach członkowskich przekazują informacje, koordynują i współpracują z właściwym organem, o którym mowa w art. 17 ust. 1 lit. c) i d), w odniesieniu do środków wprowadzonych na podstawie art. 6 i działań w zakresie egzekwowania prawa na podstawie art. 18. Państwa członkowskie dopilnowują, by właściwy organ, o którym mowa w art. 17 ust. 1 lit. c) i d), posiadał wszystkie istotne informacje. W tym celu państwa członkowskie powinny zapewnić odpowiednie ***i bezpieczne*** kanały komunikacji lub mechanizmy umożliwiające szybką wymianę istotnych informacji. **[Popr. 113]**

3. Państwa członkowskie ~~i dostawcy usług hostingowych~~ mogą zdecydować się na wykorzystanie specjalnych narzędzi, w tym~~, w stosownych przypadkach,~~ narzędzi ustanowionych przez ~~odpowiednie organy Unii, takie jak~~ Europol, w celu ułatwienia w szczególności: **[Popr. 114]**

a) przetwarzania i informacji zwrotnych dotyczących nakazów usunięcia na podstawie art. 4;

~~b) przetwarzania i informacji zwrotnych dotyczących zgłoszeń na podstawie art. 5;~~ **[Popr. 115]**

c) współpracy w celu określenia i wdrożenia ~~proaktywnych~~***szczególnych*** środków na podstawie art. 6. **[Popr. 116]**

4. W przypadku gdy dostawcy usług hostingowych dowiedzą się o ~~jakichkolwiek dowodach przestępstw~~***jakichkolwiek treściach*** terrorystycznych, niezwłocznie informują organy odpowiedzialne za prowadzenie śledztw i ściganie przestępstw w zainteresowanym państwie członkowskim***. Jeżeli nie ma możliwości zidentyfikowania zainteresowanego państwa członkowskiego, dostawca usług hostingowych powiadamia*** ~~lub~~ punkt kontaktowy w danym państwie członkowskim na podstawie art. ~~1~~**4*1*7** ust. 2, w którym mają swoje główne miejsce prowadzenia działalności lub przedstawiciela prawnego~~. W razie wątpliwości dostawcy usług hostingowych mogą przekazać~~***, a także przekazują*** te informacje Europolowi na potrzeby odpowiednich działań następczych. **[Popr. 117]**

4a. Dostawcy usług hostingowych współpracują z właściwymi organami. **[Popr. 118]**

Artykuł 14

Punkty kontaktowe

1. Dostawcy usług hostingowych***, którzy wcześniej otrzymali co najmniej jeden nakaz usunięcia,*** ustanawiają punkt kontaktowy umożliwiający odbiór nakazów usunięcia ~~i zgłoszeń~~ za pomocą środków elektronicznych oraz zapewniają ich ~~szybkie~~ ***niezwłoczne*** przetwarzanie na podstawie art. 4 ~~i 5~~. Dopilnowują oni, aby informacje na ten temat były publicznie dostępne. **[Popr. 119]**

2. W informacjach, o których mowa w ust. 1, określa się język lub języki urzędowe Unii, o których mowa w rozporządzeniu 1/58, w których można zwracać się do punktu kontaktowego i w których odbywają się dalsze wymiany informacji w związku z nakazami usunięcia ~~i zgłoszeniami~~ na podstawie art. 4 ~~i 5~~. Obejmują one co najmniej jeden z języków urzędowych państwa członkowskiego, w którym dostawca usług hostingowych ma swoje główne miejsce prowadzenia działalności lub w którym mieszka lub ma miejsce prowadzenia działalności jego przedstawiciel prawny na mocy art. 16. **[Popr. 120]**

~~3. Państwa członkowskie ustanawiają punkt kontaktowy, który będzie obsługiwać wnioski o wyjaśnienia i informacje zwrotne dotyczące wydanych przez nie nakazów usunięcia i dokonanych zgłoszeń. Informacje na temat punktu kontaktowego są publicznie dostępne.~~ **[Popr. 121]**

Środa, 17 kwietnia 2019 r.

SEKCJA V

WDROŻENIE I EGZEKWOWANIE

Artykuł 15

Jurysdykcja

1. Państwo członkowskie, w którym znajduje się główne miejsce prowadzenia działalności dostawcy usług hostingowych, ma jurysdykcję do celów art. 6, 18 i 21. Uznaje się, że dostawca usług hostingowych, który nie ma swojego głównego miejsca prowadzenia działalności w jednym z państw członkowskich, podlega jurysdykcji państwa członkowskiego, w którym mieszka lub ma miejsce prowadzenia działalności przedstawiciel prawny, o którym mowa w art. 16.

2. W przypadku gdy dostawca usług hostingowych, ***którego główne miejsce prowadzenia działalności nie mieści się w jednym z państw członkowskich,*** nie wyznaczy przedstawiciela prawnego, jurysdykcję mają wszystkie państwa członkowskie. ***Jeśli państwo członkowskie postanowi skorzystać z tej jurysdykcji, informuje o tym wszystkie pozostałe państwa członkowskie.*** **[Popr. 122]**

~~3. W przypadku gdy organ innego państwa członkowskiego wydał nakaz usunięcia zgodnie z art. 4 ust. 1, to państwo członkowskie ma jurysdykcję do zastosowania środków przymusu zgodnie ze swoim prawem krajowym w celu wykonania nakazu usunięcia.~~ **[Popr. 123]**

Artykuł 16

Przedstawiciel prawny

1. Dostawca usług hostingowych, który nie ma miejsca prowadzenia działalności w Unii, ale oferuje usługi w Unii, wyznacza na piśmie osobę prawną lub fizyczną jako swojego przedstawiciela prawnego w Unii w celu odbioru, stosowania się do i wykonywania nakazów usunięcia~~, zgłoszeń, wniosków i~~ ***i*** decyzji wydanych przez właściwe organy na podstawie niniejszego rozporządzenia. Przedstawiciel prawny rezyduje lub ma siedzibę w jednym z państw członkowskich, w których dostawca usług hostingowych oferuje swoje usługi. **[Popr. 124]**

2. Dostawca usług hostingowych powierza przedstawicielowi prawnemu odbiór, stosowanie się do i wykonywanie nakazów usunięcia, ~~zgłoszeń, wniosków~~ i decyzji, o których mowa w ust. 1, w imieniu tego dostawcy usług hostingowych. Dostawcy usług hostingowych przekazują swojemu przedstawicielowi prawnemu uprawnienia i zasoby niezbędne do współpracy z właściwymi organami oraz stosowania się do tych decyzji i nakazów. **[Popr. 125]**

3. Wyznaczony przedstawiciel prawny może zostać pociągnięty do odpowiedzialności z tytułu niewywiązania się z obowiązków wynikających z niniejszego rozporządzenia, bez uszczerbku dla odpowiedzialności dostawcy usług hostingowych i postępowań sądowych, które mogą zostać wszczęte przeciwko dostawcy usług hostingowych.

4. Dostawca usług hostingowych powiadamia o wyznaczeniu przedstawiciela prawnego właściwy organ, o którym mowa w art. 17 ust. 1 lit. d), w państwie członkowskim, w którym mieszka lub ma miejsce prowadzenia działalności przedstawiciel prawny. Informacje na temat przedstawiciela prawnego są publicznie dostępne.

SEKCJA VI

PRZEPISY KOŃCOWE

Artykuł 17

Wyznaczenie właściwych organów

1. Każde państwo członkowskie wyznacza właściwy organ ***sądowy*** lub ~~organy~~***funkcjonalnie niezależny organ administracyjny*** na potrzeby: **[Popr. 126]**

a) wydawania nakazów usunięcia na podstawie art. 4;

Środa, 17 kwietnia 2019 r.

~~b) wykrywania, identyfikacji i zgłaszania treści o charakterze terrorystycznym dostawcom usług hostingowych na podstawie art. 5;~~ **[Popr. 127]**

c) nadzoru nad wdrażaniem ~~proaktywnych~~***szczególnych*** środków na podstawie art. 6; **[Popr. 128]**

d) egzekwowania obowiązków na podstawie niniejszego rozporządzenia poprzez nakładanie sankcji na podstawie art. 18.

1a. Państwa członkowskie wyznaczają w ramach właściwych organów punkt kontaktowy, który będzie obsługiwać wnioski o wyjaśnienia i informacje zwrotne dotyczące wydanych przez nie nakazów usunięcia. Informacje na temat punktu kontaktowego są publicznie dostępne. **[Popr. 129]**

2. Najpóźniej do dnia [*sześć miesięcy po wejściu w życie niniejszego rozporządzenia*] państwa członkowskie powiadamiają Komisję o właściwych organach, o których mowa w ust. 1. Komisja ***tworzy internetowy rejestr zawierający wykaz wszystkich właściwych organów i wyznaczonych punktów kontaktowych dla każdego właściwego organu. Komisja*** publikuje to powiadomienie oraz wszelkie jego zmiany w *Dzienniku Urzędowym Unii Europejskiej*. **[Popr. 130]**

Artykuł 18

Sankcje

1. Państwa członkowskie ustanawiają zasady dotyczące sankcji mających zastosowanie w przypadku ***systematycznego i ciągłego*** niewypełniania obowiązków na podstawie niniejszego rozporządzenia przez dostawców usług hostingowych i wprowadzają wszelkie niezbędne środki w celu zapewnienia ich wdrożenia. Sankcje takie ograniczają się do przypadków niewypełnienia obowiązków wynikających z: **[Popr. 131]**

~~a) art. 3 ust. 2 (warunki dostawców usług hostingowych);~~ **[Popr. 132]**

b) art. 4 ust. 2 i 6 (wdrożenie i informacja zwrotna na temat nakazów usunięcia);

~~c) art. 5 ust. 5 i 6 (ocena i informacja zwrotna na temat zgłoszeń);~~ **[Popr. 133]**

d) art. 6 ust. ~~2 i~~ 4 (sprawozdania na temat proaktywnych środków oraz przyjęcie środków w następstwie ***wniosku***~~decyzji~~ o narzuceniu ~~szczególnych proaktywnych~~ ***dodatkowych szczególnych*** środków); **[Popr. 134]**

e) art. 7 (zachowywanie danych);

f) art. 8 (przejrzystość ***w odniesieniu do dostawców usług hostingowych***); **[Popr. 135]**

g) art. 9 (gwarancje ~~w odniesieniu do proaktywnych~~ ***dotyczące wdrażania szczególnych*** środków); **[Popr. 136]**

h) art. 10 (procedury rozpatrywania skarg);

i) art. 11 (informacje dla dostawców treści);

j) art. 13 ust. 4 (informacje na temat ~~dowodów popełnienia przestępstw~~***treści*** terrorystycznych); **[Popr. 137]**

k) art. 14 ust. 1 (punkty kontaktowe);

l) art. 16 (wyznaczenie przedstawiciela prawnego).

2. ~~Przewidziane sankcje~~***Sankcje zgodne z ust. 1*** muszą być skuteczne, proporcjonalne i odstraszające. Państwa członkowskie najpóźniej do dnia … [*w ciągu sześciu miesięcy od wejścia w życie niniejszego rozporządzenia*] r. powiadamiają Komisję o tych przepisach i środkach, a następnie niezwłocznie powiadamiają ją o wszelkich zmianach mających wpływ na te przepisy. **[Popr. 138]**

3. Państwa członkowskie zapewniają, by przy ustalaniu rodzaju i wysokości sankcji właściwe organy uwzględniały wszystkie istotne okoliczności, w tym:

a) charakter, wagę i czas trwania naruszenia;

b) umyślny lub wynikający z zaniedbania charakter naruszenia;

c) wcześniejsze naruszenia popełnione przez pociąganą do odpowiedzialności osobę prawną;

d) kondycja finansowa pociąganej do odpowiedzialności osoby prawnej;

e) poziom współpracy dostawcy usług hostingowych z właściwymi organami.**; [Popr. 139]**

ea) charakter i wielkość dostawców usług hostingowych, szczególnie w przypadku mikroprzedsiębiorstw i małych przedsiębiorstw w rozumieniu zalecenia Komisji 2003/361/WE ([13]). [Popr. 140]

4. Państwa członkowskie zapewniają, aby systematyczne ***i ciągłe*** niedopełnianie obowiązków wynikających z art. 4 ust. 2 podlegało sankcjom finansowym w wysokości do 4 % całkowitych obrotów dostawcy usług hostingowych w ostatnim roku obrotowym. **[Popr. 141]**

Artykuł 19

Wymogi techniczne***, kryteria oceny znacznej liczby nakazów*** i zmiany szablonów nakazów usunięcia **[Popr. 142]**

1. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 20 w celu uzupełnienia niniejszego rozporządzenia o ***niezbędne*** wymogi techniczne dotyczące środków elektronicznych, które mają być stosowane przez właściwe organy do przekazywania nakazów usunięcia. **[Popr. 143]**

***1a. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 20, aby uzupełnić niniejsze rozporządzenie za pomocą kryteriów i liczb, z których właściwe organy będą korzystać, aby określać, co oznacza znaczna liczba niepodważanych nakazów usunięcia, o której mowa w niniejszym rozporządzeniu.* [Popr. 144]**

2. Komisja jest uprawniona do przyjmowania takich aktów delegowanych w celu wprowadzenia zmian w załącznikach I, II i III, by skutecznie zrealizować ewentualną potrzebę poprawienia treści formularzy nakazu usunięcia oraz formularzy wykorzystywanych do przekazywana informacji na temat niemożliwości wykonania nakazu usunięcia.

Artykuł 20

Wykonywanie przekazanych uprawnień

1. Powierzenie Komisji uprawnień do przyjęcia aktów delegowanych podlega warunkom określonym w niniejszym artykule.

2. Uprawnienia do przyjęcia aktów delegowanych, o których mowa w art. 19, powierza się Komisji na czas nieokreślony od dnia [*data stosowania niniejszego rozporządzenia*] r.

3. Przekazanie uprawnień, o którym mowa w art. 19, może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna od następnego dnia po jej opublikowaniu w Dzienniku Urzędowym Unii Europejskiej lub w określonym w tej decyzji późniejszym terminie. Nie wpływa ona na ważność jakichkolwiek już obowiązujących aktów delegowanych.

4. Przed przyjęciem aktu delegowanego Komisja konsultuje się z ekspertami wyznaczonymi przez każde państwo członkowskie zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym w sprawie lepszego stanowienia prawa z dnia 13 kwietnia 2016 r.

([13]) Zalecenie Komisji z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw, małych i średnich przedsiębiorstw (Dz.U. L 124 z 20.5.2003, s. 36).

5. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie.

6. Akt delegowany przyjęty na podstawie art. 19 wchodzi w życie tylko wówczas, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie dwóch miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie lub gdy przed upływem tego terminu zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o dwa miesiące z inicjatywy Parlamentu Europejskiego lub Rady.

Artykuł 21

Monitorowanie

1. Państwa członkowskie gromadzą od swoich właściwych organów i dostawców usług hostingowych podlegających ich jurysdykcji i co roku przesyłają Komisji do dnia [31 marca] informacje na temat działań, które podjęli zgodnie z niniejszym rozporządzeniem. Informacje te obejmują:

a) informacje o liczbie wydanych nakazów usunięcia ~~i dokonanych zgłoszeń~~, o liczbie przypadków usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do nich, wraz z odpowiednimi ramami czasowymi na podstawie art. 4 ***, oraz informacje o liczbie związanych z nimi przypadków skutecznego wykrycia przestępstw terrorystycznych, prowadzenia dochodzeń w ich sprawie*** i ~~5~~***ich ścigania***; **[Popr. 145]**

b) informacje dotyczące szczególnych proaktywnych środków wprowadzonych na podstawie art. 6, w tym ilości treści o charakterze terrorystycznym, które zostały usunięte lub do których dostęp został uniemożliwiony, oraz odpowiednie ramy czasowe;

ba) informacje o liczbie wniosków o dostęp wydanych przez właściwe organy w odniesieniu do treści zachowywanych przez dostawcę usług hostingowych zgodnie z art. 7; **[Popr. 146]**

c) informacje dotyczące liczby wszczętych procedur rozpatrywania skarg oraz działań podjętych przez dostawców usług hostingowych na podstawie art. 10;

d) informacje dotyczące liczby wszczętych procedur odwoławczych oraz decyzji podjętych przez właściwy organ zgodnie z prawem krajowym.

2. Najpóźniej do dnia [*rok po dniu rozpoczęcia stosowania niniejszego rozporządzenia*] r. Komisja ustala szczegółowy program monitorowania produktów, rezultatów i skutków niniejszego rozporządzenia. W programie monitorowania określa się wskaźniki i środki służące do gromadzenia danych i innych niezbędnych dowodów, a także przedziały czasowe, w jakich mają one być gromadzone. Określa się w nim działania, które mają zostać podjęte przez Komisję i państwa członkowskie przy gromadzeniu i analizowaniu danych i innych dowodów w celu monitorowania postępów i dokonania oceny niniejszego rozporządzenia na podstawie art. 23.

Artykuł 22

Sprawozdanie z wdrażania

Do dnia [*dwa lata po wejściu w życie niniejszego rozporządzenia*] r. Komisja składa Parlamentowi Europejskiemu i Radzie sprawozdanie ze stosowania niniejszego rozporządzenia. Informacje dotyczące monitorowania na podstawie art. 21 oraz informacje wynikające z obowiązków w zakresie przejrzystości na podstawie art. 8 są uwzględniane w sprawozdaniu Komisji. Państwa członkowskie przekazują Komisji informacje niezbędne do przygotowania sprawozdania.

Artykuł 23

Ocena

~~Nie wcześniej niż w dniu [*trzy lata*~~***Rok*** od daty rozpoczęcia stosowania niniejszego rozporządzenia~~]~~ ~~r.~~ Komisja dokonuje oceny niniejszego rozporządzenia i przedstawia Parlamentowi Europejskiemu i Radzie sprawozdanie dotyczące stosowania niniejszego rozporządzenia, w tym skuteczności funkcjonowania mechanizmów ochronnych ***oraz oddziaływania na poszanowanie praw podstawowych, w tym wolności wypowiedzi oraz wolności otrzymywania i przekazywania informacji, a także prawa do poszanowania życia prywatnego. W kontekście tej oceny Komisja zdaje też sprawę z konieczności, wykonalności i skuteczności utworzenia Europejskiej Platformy ds. Treści o Charakterze Terrorystycznym***

w Internecie, która umożliwiałaby wszystkim państwom członkowskim korzystanie z jednego, bezpiecznego kanału komunikacji, aby przesyłać nakazy usunięcia treści o charakterze terrorystycznym do dostawców usług hostingowych. W stosownych przypadkach sprawozdaniu towarzyszą wnioski ustawodawcze. Państwa członkowskie przekazują Komisji informacje niezbędne do przygotowania sprawozdania. **[Popr. 147]**

Artykuł 24

Wejście w życie

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Rozporządzenie stosuje się od dnia [~~6~~**12** miesięcy po wejściu w życie] r. **[Popr. 148]**

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia […] r.

W imieniu Parlamentu Europejskiego *Przewodniczący*

W imieniu Rady *Przewodniczący*

Środa, 17 kwietnia 2019 r.

ZAŁĄCZNIK I

NAKAZ USUNIĘCIA TREŚCI O CHARAKTERZE TERRORYSTYCZNYM (art. 4 rozporządzenia (UE) xxx)

Na podstawie art. 4 rozporządzenia (UE) … [1] adresat nakazu usunięcia usuwa treści o charakterze terrorystycznym lub uniemożliwia dostęp do nich w ciągu jednej godziny od otrzymania nakazu usunięcia od właściwego organu.

Zgodnie z art. 7 rozporządzenia (UE) … [2] adresaci muszą zachować treści i związane z nimi dane, które zostały usunięte lub do których dostęp uniemożliwiono, przez okres co najmniej sześciu miesięcy na wniosek właściwych organów lub sądów.

Nakaz usunięcia należy wysłać w jednym z języków wskazanych przez adresata na podstawie art. 14 ust. 2.

SEKCJA A:

Państwo członkowskie wydające nakaz: . . . . . .

UWAGA: dane organu wydającego należy podać na końcu (sekcje E i F)

Adresat (przedstawiciel prawny):

. . . . . .

Adresat (punkt kontaktowy):

. . . . . .

Państwo członkowskie, którego jurysdykcji podlega adresat [jeśli inne niż państwo wydające nakaz]: . . . . . .

Godzina i data wydania nakazu usunięcia:

. . . . . .

Numer referencyjny nakazu usunięcia: . . . . . .

[1] Rozporządzenie Parlamentu Europejskiego i Rady w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym (*Dz.U. L …*).

[2] Rozporządzenie Parlamentu Europejskiego i Rady w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym (*Dz.U. L …*).

SEKCJA B: Treści, które mają zostać usunięte lub do których dostęp ma zostać uniemożliwiony ~~w ciągu jednej godziny:~~, ***bez zbędnej zwłoki***: **[Popr. 162]**

Adres URL i wszelkie dodatkowe informacje umożliwiające identyfikację i dokładną lokalizację treści, o których mowa:

. . . . . .

Powody, dla których treści uznaje się za treści o charakterze terrorystycznym zgodnie z art. 2 ust. 5 rozporządzenia (UE) xxx. Treści (proszę zaznaczyć właściwe pola):

☐ podżegają~~, nakłaniają~~ do popełniania przestępstw terrorystycznych ~~lub gloryfikują je~~ ***wymienionych w art. 3 ust. 1 lit. a) – i) dyrektywy (UE) 2017/541*** (art. 2 ust. 5 lit. a)); **[Popr. 149]**

☐ zachęcają ***osoby lub grupy osób*** do ~~wspierania~~ ***popełniania*** przestępstw terrorystycznych ***wymienionych w art. 3 ust. 1 lit. a) – i) dyrektywy (UE) 2017/541*** (art. 2 ust. 5 lit. ~~b~~***a***)); **[Popr. 150]**

☐ ~~propagują działalność~~ ***…] zachęcają osoby lub*** grupy ~~terrorystycznej, zachęcają~~***osób*** do udziału w ~~grupie lub jej wspierania~~ ***działaniach grupy terrorystycznej wymienionych w art. 3 ust. 1 lit. a) – i) dyrektywy (UE) 2017/541*** (art. 2 ust. 5 lit. c)); **[Popr. 151]**

☐ przedstawiają instrukcje lub techniki ~~popełniania~~***wytwarzania lub stosowania materiałów wybuchowych, broni palnej lub innych rodzajów broni lub substancji trujących lub niebezpiecznych lub w zakresie innych konkretnych metod i technik do celów popełnienia*** przestępstw terrorystycznych ***wymienionych w art. 3 ust. 1 lit. a) – i) dyrektywy (UE) 2017/541*** (art. 2 ust. 5 lit. d)); **[Popr. 152]**

☐ ***przedstawiają popełnianie przestępstw terrorystycznych wymienionych w art. 3 ust. 1 lit. a) – i) dyrektywy (UE) 2017/541 (art. 2 ust. 5 lit. e));*** **[Popr. 153]**

Dodatkowe informacje dotyczące powodów uznania treści za treści o charakterze terrorystycznym (opcjonalne):

. . . . . .

. . . . . .

SEKCJA C: Informowanie dostawcy treści

Uwaga (proszę zaznaczyć, jeżeli dotyczy):

☐ ze względów bezpieczeństwa publicznego adresat **musi powstrzymać się od informowania dostawcy treści**, którego treści są usuwane lub do którego treści dostęp uniemożliwiono.

W innych przypadkach: szczegóły dotyczące możliwości zaskarżenia nakazu usunięcia w państwie członkowskim wydającym nakaz (które można przekazać dostawcy treści na jego wniosek) na mocy prawa krajowego, zob. sekcja G poniżej:

SEKCJA D: Informowanie państwa członkowskiego, którego jurysdykcji podlega adresat

☐ Proszę zaznaczyć, jeśli państwo, którego jurysdykcji podlega adresat, jest inne niż państwo członkowskie wydające nakaz:

☐ kopia nakazu usunięcia jest przekazywana odpowiedniemu właściwemu organowi państwa, którego jurysdykcji podlega adresat

Środa, 17 kwietnia 2019 r.

SEKCJA E: Dane organu, który wydał nakaz usunięcia

Rodzaj organu, który wydał niniejszy nakaz usunięcia (proszę zaznaczyć właściwe pole):

☐ sędzia, sąd lub sędzia śledczy

☐ organ ścigania

☐ inny właściwy organ → proszę wypełnić również sekcję (F)

Dane organu wydającego nakaz lub jego przedstawiciela potwierdzające prawdziwość i poprawność nakazu usunięcia:

Nazwa organu: . . . . . .

Imię i nazwisko przedstawiciela: . . . . . .

Zajmowane stanowisko (tytuł/stopień): . . . . . .

Sygnatura sprawy: . . . . . .

Adres:

Numer telefonu: (nr kierunkowy państwa) (nr kierunkowy miejscowości) . . . . . .

Numer faksu: (nr kierunkowy państwa) (nr kierunkowy miejscowości) . . . . . .

E-mail: . . . . . .

Data:

. . . . . .

Pieczęć urzędowa (jeżeli jest dostępna) i podpis: [1] . . . . . .

SEKCJA F: Dane kontaktowe na potrzeby dalszych działań

Dane kontaktowe organu wydającego nakaz umożliwiające uzyskanie informacji zwrotnych na temat terminu usunięcia lub uniemożliwienia dostępu lub uzyskanie dalszych wyjaśnień:

. . . . . .

Dane kontaktowe organu państwa, którego jurysdykcji podlega adresat [jeżeli jest to inne państwo niż państwo członkowskie wydające nakaz]:

. . . . . .

SEKCJA G: Informacje na temat środków odwoławczych

Informacje na temat właściwego organu lub sądu, terminów i procedur***, w tym wymogów formalnych,*** zaskarżenia nakazu usunięcia: **[Popr. 154]**

Organ lub sąd właściwe do celów zaskarżenia nakazu usunięcia:

. . . . . .

Termin zaskarżenia decyzji:

XXX miesięcy, począwszy od xxxx

Link do przepisów krajowych:

. . . . . .

[1] Złożenie podpisu może nie być konieczne w przypadku wysyłania z wykorzystaniem uwierzytelnionych kanałów przekazywania informacji.

ZAŁĄCZNIK II

FORMULARZ INFORMACJI ZWROTNYCH PO USUNIĘCIU TREŚCI O CHARAKTERZE TERRORYSTYCZNYM LUB UNIEMOŻLIWIENIU DOSTĘPU DO NICH

(art. 4 ust. 5 rozporządzenia (UE) xxx)

SEKCJA A:

Adresat nakazu usunięcia:

…….. . . . . .

Organ, który wydał nakaz usunięcia:

…….. . . . . .

Sygnatura sprawy nadana przez organ wydający nakaz:

…….. . . . . .

Sygnatura sprawy nadana przez adresata:

…….. . . . . .

Godzina i data otrzymania nakazu usunięcia:

…….. . . . . .

SEKCJA B:

Treści o charakterze terrorystycznym objęte nakazem usunięcia / dostęp do treści o charakterze terrorystycznym objętych nakazem usunięcia (proszę zaznaczyć właściwe pole):

☐ został usunięte

☐ został uniemożliwiony

Data i godzina usunięcia lub uniemożliwienia dostępu: …….. . . . . .

SEKCJA C: Dane dotyczące adresata

Nazwa dostawcy usług hostingowych / przedstawiciela prawnego:

…….. . . . . .

Państwo członkowskie głównego miejsca prowadzenia działalności lub miejsca prowadzenia działalności przedstawiciela prawnego: …….. . . . . .

Imię i nazwisko osoby upoważnionej:

…….. . . . . .

Dane punktu kontaktowego (e-mail): ……. . . . . .

Data:

…….. . . . . .

Środa, 17 kwietnia 2019 r.

ZAŁĄCZNIK III

INFORMACJE NA TEMAT NIEMOŻLIWOŚCI WYKONANIA NAKAZU USUNIĘCIA (art. 4 ust. 6 i 7 rozporządzenia (UE) xxx)

SEKCJA A:

Adresat nakazu usunięcia:

……..…….. . . . . .

Organ, który wydał nakaz usunięcia:

……..…….. . . . . .

Sygnatura sprawy nadana przez organ wydający nakaz:
……..…….. . . . . .

Sygnatura sprawy nadana przez adresata: ……..
……... . . . . .

Godzina i data otrzymania nakazu usunięcia:

……..…….. . . . . .

SEKCJA B: Podstawy niewykonania

(i) Nakaz usunięcia nie może zostać wykonany lub nie może zostać wykonany w żądanym terminie z następującego (-ych) powodu(-ów):

☐ siła wyższa lub faktyczna niemożliwość, których nie można przypisać adresatowi lub dostawcy usług***, w tym z powodów technicznych lub operacyjnych*** **[Popr. 155]**

☐ nakaz usunięcia zawiera oczywiste błędy

☐ nakaz usunięcia nie zawiera wystarczających informacji

(ii) Proszę podać dalsze informacje dotyczące powodów niewykonania:

…….. . . . . .

(iii) Jeżeli nakaz usunięcia zawiera oczywiste błędy lub nie zawiera wystarczających informacji, proszę określić, jakie to są błędy, oraz proszę podać, jakie dalsze informacje lub wyjaśnienia są wymagane:

…….. . . . . .

SEKCJA H: Dane dostawcy usług / przedstawiciela prawnego

Nazwa dostawcy usług / przedstawiciela prawnego:

……..…….. . . . . .

Imię i nazwisko osoby upoważnionej:

……..…….. . . . . .

Dane kontaktowe (e-mail):

……..…….. . . . . .

Podpis:

……..…….. . . . . .

Godzina i data: ……..…….. . . . . .